



EU CYBER VAT

Fighting cyber-VAT fraud in the EU:
a comparative criminological
and criminal law study

Final Report

**Andrea Di Nicola, Roberto Flor, Gabriele Baratto,
Denise Boriero, Giulia Perrone, Beatrice Panattoni**
Centre for Security and Crime Sciences (CSSC)
University of Trento and University of Verona (Italy)



Co-funded by
the European Union

EU CYBER VAT - Final Report

Authors:

Andrea Di Nicola
Roberto Flor
Gabriele Baratto
Denise Boriero
Giulia Perrone
Beatrice Panattoni

*The **research team** included (in alphabetical order): Gabriele Baratto, Caterina Bergomi, Denise Boriero, Silvia Civitella, Andrea Di Nicola, Roberto Flor, Elena Ioriatti, Beatrice Panattoni, Giulia Perrone, Beatrice Rigon, Ludovica Tomasini. With the support of: Sofia Carroccia, Chiara Dordolo, Rita Viviani*

Project: EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study

Deliverable D3.2

Beneficiary



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Anti-Fraud Office (OLAF). Neither the European Union nor the granting authority can be held responsible for them.

Centre for Security and Crime Sciences (CSSC) of the University of Trento and the University of Verona
www.cssc.unitn.it

Trento, July 2025

© CSSC – Università degli Studi di Trento

Table of contents

1. Introduction	7
1.1 Background.....	7
1.2 Scope and methodology.....	11
 2. Cyber-VAT fraud in the European Union: an empirical criminological analysis and the role of technologies.....	15
2.1 Objective and aim	15
2.2 Research design and methods.....	16
2.3 The analysis.....	18
<i>Clusters of modus operandi and actors</i>	<i>18</i>
<i>The role of ICTs: script analysis and interpretation.....</i>	<i>22</i>
2.4 Concluding remarks.....	26
 3. Pif Directive (Directive 2017/1371/EU) and its implementation in the Member States.....	28
3.1 National legislations	29
<i>Austria</i>	<i>29</i>
<i>Belgium.....</i>	<i>32</i>
<i>Bulgaria</i>	<i>34</i>
<i>Croatia</i>	<i>36</i>
<i>Cyprus.....</i>	<i>38</i>
<i>Czech Republic.....</i>	<i>38</i>
<i>Denmark.....</i>	<i>40</i>
<i>Estonia.....</i>	<i>41</i>
<i>Finland.....</i>	<i>42</i>
<i>France.....</i>	<i>43</i>
<i>Germany.....</i>	<i>46</i>
<i>Greece</i>	<i>50</i>
<i>Hungary.....</i>	<i>52</i>
<i>Ireland.....</i>	<i>55</i>
<i>Italy.....</i>	<i>56</i>
<i>Latvia.....</i>	<i>59</i>
<i>Lithuania.....</i>	<i>63</i>
<i>Luxembourg.....</i>	<i>66</i>
<i>Malta</i>	<i>67</i>

<i>The Netherlands</i>	68
<i>Poland</i>	71
<i>Portugal</i>	72
<i>Romania</i>	74
<i>Slovakia</i>	76
<i>Slovenia</i>	77
<i>Spain</i>	79
<i>Sweden</i>	83
3.2 General considerations and concluding remarks.....	84
<i>Compliance with Article 3 of the PIF Directive</i>	84
<i>Objective element of the VAT-related offenses</i>	86
<i>Subjective element of the VAT-related offenses</i>	88
<i>Compliance with Article 7 of the PIF Directive</i>	90
<i>Aggravating circumstances for VAT fraud committed within a criminal organisation</i>	91
<i>Compliance with Article 6 of the PIF Directive</i>	92
<i>Sanctions with regard to legal persons</i>	94
4. National criminal law systems and cyber-VAT fraud: similarities and differences between the relevant national legislations of the Member States	95
4.1 National legislations	96
<i>Austria</i>	96
<i>Belgium</i>	96
<i>Bulgaria</i>	97
<i>Croatia</i>	97
<i>Cyprus</i>	97
<i>Czech Republic</i>	98
<i>Denmark</i>	98
<i>Estonia</i>	98
<i>Finland</i>	98
<i>France</i>	98
<i>Germany</i>	98
<i>Greece</i>	99
<i>Hungary</i>	99
<i>Italy</i>	99
<i>Latvia</i>	100
<i>Lithuania</i>	100
<i>Luxembourg</i>	100
<i>Malta</i>	100

<i>The Netherlands</i>	100
<i>Poland</i>	101
<i>Portugal</i>	101
<i>Slovakia</i>	101
<i>Slovenia</i>	101
<i>Spain</i>	101
<i>Sweden</i>	102
4.2 Considerations concerning a possible autonomous offence	102

5. Combating cyber-VAT fraud and criminal investigations: similarities and differences between the relevant national legislations of the Member States 105

5.1 Investigative tools against cyber-VAT fraud.....	105
5.2 National legislations	108
<i>Austria</i>	108
<i>Belgium</i>	109
<i>Bulgaria</i>	114
<i>Croatia</i>	116
<i>Cyprus</i>	119
<i>Czech Republic</i>	120
<i>Denmark</i>	122
<i>Estonia</i>	122
<i>Finland</i>	123
<i>France</i>	123
<i>Germany</i>	124
<i>Greece</i>	126
<i>Hungary</i>	127
<i>Ireland</i>	128
<i>Italy</i>	130
<i>Latvia</i>	131
<i>Lithuania</i>	133
<i>Luxembourg</i>	135
<i>Malta</i>	136
<i>The Netherlands</i>	137
<i>Poland</i>	138
<i>Portugal</i>	139
<i>Romania</i>	139
<i>Slovakia</i>	142
<i>Slovenia</i>	142

Spain	143
Sweden.....	146
6. E-commerce and cooperation between the public and private sectors to combat and prevent cyber-VAT fraud	148
6.1 Digital marketplaces and the liability of providers	149
6.2 National legislations	153
Austria	153
Belgium.....	153
Bulgaria	155
Croatia	156
Cyprus.....	156
Czech Republic.....	157
Denmark.....	159
Estonia.....	160
Finland.....	160
France.....	161
Germany.....	161
Greece	162
Hungary.....	163
Ireland.....	163
Italy.....	164
Latvia.....	165
Lithuania.....	166
Luxembourg.....	167
Malta	167
The Netherlands.....	168
Poland.....	169
Portugal	170
Romania	171
Slovakia	172
Slovenia.....	174
Spain	174
Sweden.....	175
6.3 Anti-fraud cycle and the role of the private sector in combating and preventing cyber-VAT fraud VAT.....	176

7. Recommendations and proposals to improve anti-fraud strategies against cyber-VAT fraud	178
7.1 Substantive criminal law	178
<i>Harmonisation, legal convergence and integration in the EU</i>	178
<i>Regulatory reforms</i>	180
7.2 Criminal procedure and investigations	181
<i>Specialised and more efficient investigations</i>	181
<i>Use of technology in prevention and investigations</i>	183
<i>Effective use of reporting systems</i>	184
<i>Judicial cooperation</i>	185
7.3 Payment service providers and platform obligations	187
7.4 Concluding remarks.....	188
7.5 Recommendations Summary.....	190
 Bibliography.....	 192
 Annex I – Questionnaire for national experts.....	 198
 Annex II – National provisions Compliance to Art. 3 of the Directive (EU) 2017/1371 (Questionnaire Appendix 1).....	 209
 Annex III – National provisions Compliance to Art. 7 of the Directive (EU) 2017/1371 (Questionnaire Appendix 2).....	 234
 Annex IV – National provisions Compliance to Art. 6 of the Directive (EU) 2017/1371 (Questionnaire Appendix 3).....	 251

1. Introduction

1.1 Background

Value Added Tax (VAT) fraud has long been a significant issue **affecting the economies of both individual countries and the European Union (EU)**¹. As one of the most crucial sources of public revenue, VAT is essential for financing public services, sustaining the EU budget, and facilitating cross-border trade in the EU internal market. Despite its importance, VAT fraud remains a persistent challenge that undermines the financial integrity of the EU² and the Member States (MSs). In fact, VAT fraud is often seen as a serious threat to public finances due to its widespread occurrence and its capacity to distort the proper functioning of the tax system.

From a criminological perspective, VAT fraud encompasses a variety of schemes that exploit the VAT system, broadly categorized according to their objective: reducing tax liability (tax evasion) or misappropriation of VAT through non-payment or false claims for tax credits (Fedeli et al., 2011). These frauds can be very complex, ranging from national cases to international operations with complicated “carousel transactions” that increase the financial damage to the national budget (Fedeli et al., 2011). The fraud becomes even more damaging when several transactions are used to create multiplier effects that cause damage to the public purse through the non-payment and deduction of VAT. The issue here is twofold: firstly, the missing trader invoices VAT to its customer but does not subsequently pay it to the tax authorities, and secondly, the customer can deduct the input VAT paid to the missing trader (Lamench, 2018).

A particularly harmful and widespread scheme in the European Union is missing trader intra-community (MTIC) fraud, a complex and often large-scale form of VAT fraud recognized by Europol (SOCTA, 2013) as one of the biggest organized crime threats in the EU. One important form of MTIC is carousel fraud (CEPOL, 2022), which can be open or closed; the ‘closed carousel’ represents the “reference form” for this type of fraud, precisely because of the circular shape from which the

¹ In the context of VAT fraud, there are numerous contributions coming from a wide range of stakeholders, including academic researchers, law enforcement agencies, and EU institutions, all of which provide valuable insights and data to better understand the nature, scale, and dynamics of VAT fraud. Among all, see for instance: M.C. Frunza, “Value Added Tax Fraud”, Routledge, 2018; S. Fedeli, F. Forte, “EU VAT Fraud”, in *European Journal of Law and Economics*, Vol. 31, n. 2, 143-166, 2009; M. Keen, S. Smith, “VAT Fraud and Evasion: What Do We Know and What Can Be Done?”, in *National Tax Journal*, Vol. 59, n. 4, 861-887, 2006.

² To better understand the European dimension of this crime, see: M. Griffioen, E.C.J.M. van der Hel-van Dijk “Tackling VAT-Fraud in Europe: A Complicated International Puzzle”, in *Intertax*, Volume 44, Issue 4, 290 – 297, 2016; L. Sergiou, “Value Added Tax (VAT) Carousel Fraud in the European Union” in *Journal of Accounting and Management*, vol. 2 n. 2, 9-21, 2012; M. Lamensch, E. Ceci, “VAT fraud - Economic impact, challenges and policy issues”, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, 2018, retrieved from: <https://www.europarl.europa.eu/cmsdata/156408/VAT%20Fraud%20Study%20publication.pdf>; F. Borselli, “Organised Vat Fraud: Features, Magnitude, Policy Perspectives”, in *Bank of Italy Occasional Paper* No. 106, 2011, retrieved from: <https://ssrn.com/abstract=1966015>; R. F. van Brederode, “Third-Party Risks and Liabilities in Case of VAT Fraud in the EU”, in *International Tax Journal*, January – February, 2008, 31-42; M. Frunza, “Cost of the MTIC VAT Fraud for European Union Members”, 2016, retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2758566; T. Michalik, “How the European Commission and European Countries Fight VAT Fraud”, mBank - CASE Seminar Proceedings 0147, CASE-Center for Social and Economic Research, 2017; J. Sarnowski, P. Selera, “European compact against tax fraud—VAT solidarity and new dimension of effective and coherent tax data transfer”, *ERA Forum* 21, 2020, p. 81-93, retrieved from: <https://doi.org/10.1007/s12027-020-00603-z>.

name 'carousel' originates. This mechanism leads to double financial losses for the state due to unpaid taxes and unjustified VAT refunds (European Parliament, 2021).

To address such growing threats, the EU established the European Public Prosecutor's Office (EPPO) in 2020, which became operational in July 2021, to tackle large-scale financial crimes affecting the EU's financial interests, such as VAT fraud, money laundering, and the misuse of EU funds.

EPPO has specific thresholds for its jurisdiction in relation to the financial impact of criminal offence. These limits are set out in Council Regulation (EU) 2017/1939, which establishes the EPPO. With regards to VAT fraud, EPPO's competence for cross-border VAT fraud if the estimated damage exceeds €10 million. This very high threshold reflects the significant financial impact of large-scale VAT fraud schemes, such as carousel fraud, on the EU's financial interests. Indeed, VAT fraud can be perpetrated by individuals on an occasional basis, by companies with established operations and substantial turnover, but it clearly becomes more significant when committed by **organised crime groups**. According to Europol, fraud in general – which includes VAT fraud – represents the second most common activity of the most threatening criminal networks: eighteen of the most dangerous criminal networks specialize in VAT fraud, including carousel fraud, and typically maintain end-to-end control over the entire criminal process.

Unpaid VAT often serves as the main source of funding for criminal organizations that specialize in this category of economic and financial crime and use the funds to finance other forms of criminal activity. This further demonstrates how VAT fraud is not merely a financial offence but part of a broader criminal economy. Despite its significant economic and social consequences, VAT fraud has been largely neglected in criminological research, which has traditionally focused on white-collar crime and corporate misconduct, leaving a gap in understanding VAT fraud as a specific criminal phenomenon.

A clear indicator of the extent and significance of VAT fraud is reflected in the EPPO's 2023 Annual Report³. The report shows that **59% of the estimated losses of €19.2 billion for the year were due to VAT fraud**, marking a dramatic 71% increase compared to 2022. This highlights VAT fraud as a complex criminal offence that usually involves large companies and affects various jurisdictions inside and outside the EU market.

The digital revolution has further exacerbated the problem, providing new tools and opportunities for fraudsters. Indeed, one of the biggest challenges in the fight against VAT fraud today is the **increasing exploitation of digital technologies by criminals**⁴. Sophisticated technologies such as

³ EPPO Annual Report 2023, retrieved from: https://www.epo.europa.eu/sites/default/files/2024-03/EPPO_Annual_Report_2023.pdf.

⁴ On digital VAT frauds, see: L. Foffani, L. Bin, M. F. Carriero, "Cyber VAT frauds, ne bis in idem and judicial cooperation, A comparative study between Italy, Belgium, Spain and Germany" – Research project, Giappichelli, 2019; J. Nicholls, A. Kuppa and N. A. Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape," in IEEE Access, vol. 9, 163965-163986, 2021; M. Lagazio, N. Sherif, N. Cushman, "A multilevel approach to understanding the impact of cybercrime in the financial sector" in Computer & Security, Vol. 45, 1-32, 2014; J. Vanhoeyveld, D. Martens, B. Peeters, "Value-Added Tax fraud detection with scalable anomaly detection techniques" in Applied Soft Computing, Vol. 86, n. , 2020; F. Borselli, S. Fedeli, L. Giuriato, "Digital VAT carousel frauds: a new boundary for criminality?", TAX NOTES INTERNATIONAL; 707-724, 2015; Papis-Almansa, "VAT and electronic commerce: the new rules as a means for simplification, combatting fraud and creating a more level playing field?", ERA Forum 20, 2019, 201–223, retrieved from: <https://doi.org/10.1007/s12027-019-00575-9>; R. T. Ainsworth, "Carousel Fraud in the EU: A Digital Vat Solution", in Tax Notes International, p. 443, May 1, 2006, Boston Univ. School of Law Working Paper No. 06-23, retrieved from: <https://ssrn.com/abstract=924189>.

cryptocurrencies, anonymous payment systems, and the growth of e-commerce now frequently enable anonymity, speed, and cross-border operations, making detection and enforcement more difficult (Lee & Holt, 2020; Borselli et al., 2015).

The dematerialization of assets and transactions complicates efforts to detect criminal activity, as authorities struggle to trace the flow of money and goods. In particular, the rise of e-commerce has enabled fraudulent companies to exploit the complexity of cross-border transactions, using methods such as false reporting, failure to register for VAT, and invalid VAT numbers to evade taxes (Moiseienko, 2020).

As ICT (Information and Communication Technology) continues to evolve, so do the tactics used by fraudsters. Digital technologies, including e-commerce platforms, blockchain anonymity, and financial technology (fintech) solutions, have opened up new avenues for fraudulent activity. Criminals are now using online payment systems, cryptocurrencies, and digital wallets to disguise illicit transactions, making detection and enforcement challenging for tax authorities⁵. In particular, the **use of online platforms** enables fraudulent traders to disguise their operations, often through cross-border schemes, creating a complex web of transactions that tax authorities struggle to trace. Furthermore, **digital invoicing systems** and the ability to create forged documents with minimal resources have further reduced the barriers to committing VAT fraud. At the same time, the use of digital tools for VAT fraud has made traditional detection methods⁶ less effective. Innovative approaches are therefore needed to tackle the cyber dimension of financial crime.

Despite the pervasive nature of these phenomena and their significant impact on the global economy, the existing body of literature on the subject—both in criminal law and criminology—remains decidedly sparse and fragmented. The phenomenon, particularly at the digital level, has yet to be comprehensively studied, and there is a clear lack of an effective and systematic mapping of the criminal law and procedural tools available to address it. This **gap** is further highlighted by the **lack of a common and uniform definition of cyber-VAT fraud**, which continues to hamper efforts to develop coordinated responses and standardized legal approaches at national and international level. Moreover, digital exploitation is complicated by the global nature of e-commerce, where VAT fraudsters often operate across borders, and take advantage of different national regulations and tax systems. This challenge is exacerbated by the fact that, as is often seen in the fight against cybercrime, national legal frameworks and enforcement measures struggle to keep pace with the rapid pace of technological advancement, leaving them unable to effectively counter these evolving threats.

To counter the emerging threat of cyber VAT fraud, it is essential to understand how digital technologies are leveraged by criminals. This understanding helps to develop more effective law enforcement strategies and facilitates the identification of best practice in combating such crimes. It also highlights the importance of cross-border cooperation between EU Member States, as well as with supranational institutions such as Europol, in order to respond quickly to the increasing complexity of financial crime. The EU's efforts to combat VAT fraud are in line with the European Commission's political guidelines for the period 2024-2029, which emphasize the strengthening

⁵ European Commission, "Combating VAT fraud", 2017, retrieved from <https://ec.europa.eu>;

⁶ For a detailed analysis of investigative tools for tackling VAT fraud, see: F. Borselli, "Pragmatic Policies to Tackle VAT Fraud in the European Union" in *International VAT Monitor*, No. 5, 332-343, September/October 2008; O. Sokolovska, "Cross-border VAT frauds and measures to tackle them", 2016, retrieved from: <https://mpr.a.ub.uni-muenchen.de/70504/> ; European Union, "Tackling intra-Community VAT fraud: More action needed", Publications Office of the European Union, 2016; CESOP - Guidelines for the reporting of payment data, 2023, retrieved from: https://taxation-customs.ec.europa.eu/taxation/vat/fight-against-vat-fraud/tackling-vat-fraud-e-commerce-cesop_en.

of the EPPO's capacities. The guidelines propose granting the EPPO additional powers and support from Europol, to develop into a fully operational police authority with increased resources⁷. This enhanced institutional cooperation will enable a more efficient and coordinated approach to tackling complex fraud and related crimes across the EU. In order to achieve these objectives, **accurate, timely, and shared data on VAT fraud in the Member States is crucial**.

This is where initiatives such as the EU CYBER VAT research project come into play. In fact, in this context, the EU Cyber VAT project has carried out an empirical criminological analysis of digital VAT fraud within the European Union, alongside a comparative legal study. It offers a detailed overview of the transposition of EU criminal law into national legislations, analyzing the differences between Member States' legal systems and identifying the most effective national best practices for preventing and combating the phenomenon. The project also aims to shed light on the new threats arising from the digitalisation of fiscal processes and their impact on the EU's financial interests, and to assess whether, and to what extent, existing EU law, its implementation by Member States, and national legal frameworks are adequate to address cyber VAT fraud. Particular attention is given to identifying potential legal and operational gaps that may hinder institutional response capacity.

Through an in-depth review of existing literature, analysis of current legislation, and consultations with national experts (mostly researchers) and stakeholders, several critical challenges have emerged, along with notable strengths. If these findings are effectively addressed and shared among relevant actors, they could make a significant contribution to mitigating the phenomenon.

Based on the main findings of the study – presented in detail in the present report – a set of **policy recommendations** is proposed for future **EU anti-fraud strategies**, along with **operational best practices** to support digital investigation activities.

These recommendations and shared best practises will also take into account relevant international and EU policy guidance in this area and provide a basis for discussion at the EU and national levels. These policy recommendations – included in this report – are intended to assist policymakers, PAs, LEAs, and other relevant stakeholders at all levels in designing efficient and effective responses to this rising crime, as well as in harmonising the various pieces of legislation and improving cooperation within Member States.

Project **EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study**.

General objective

The **general objective of EU CYBER VAT project** is to assess the adequacy of the current legal framework at EU and Member State level with regard to combating cyber-VAT fraud and to propose solutions to make it more effective and efficient at EU and Member State level. Using the method of comparative law research, the project will investigate whether the European criminal law framework for VAT fraud under the PIF Directive, its implementation by Member States, and national criminal law provisions can provide a sufficient level of legal protection against the intersection of VAT fraud and cybercrime. As

⁷ Ursula von der Leyen, Candidate for the European Commission President, EUROPE'S CHOICE - POLITICAL GUIDELINES FOR THE NEXT EUROPEAN COMMISSION 2024-2029, retrieved from: https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf.

these are cross-border and particularly serious crimes, the degree of harmonisation between national rules must always be monitored and ensured.

Specific objectives

The general objective of the project can be divided into the following 3 specific objectives (SO):

- To provide an analysis of cyber-VAT frauds in the European Union from an empirical criminological point of view, with special attention to the modus operandi as well as the characteristics of the actors involved. The new threats related to the digitalization of tax transactions will be assessed from a criminological perspective, in order to provide a basis for evaluating the adequacy of measures against cyber-VAT fraud in the EU and activities to detect and investigate cyber-VAT fraud by tax and law enforcement authorities;
- To provide an account of the transposition of EU criminal law into national legislations to specifically prevent and combat cyber-VAT fraud and an account of the differences between the relevant national legislations of the Member States as well as national best practices;
- To elaborate, from the dual perspective of substantive criminal law and criminal procedure, recommendations and proposals to improve the EU regulation and the national anti-fraud strategies (NAFS) against cyber-VAT fraud in order to address the new threats to the financial interests of the European Union in the context of the digital age. This will take particular account of MTIC in the digital marketplace, exploring the possibility of introducing forms of service provider accountability to prevent cyber-VAT fraud. It will also promote a higher level of harmonisation in the regulation of cross-border cyber-VAT fraud, especially when it occurs in the context of e-commerce activity.

Funding

Co-funded by the European Union – European Commission, Directorate-General for European Anti-Fraud Office (OLAF) – Union Anti-Fraud Programme – EUAF.

1.2 Scope and methodology

The EU CYBER VAT project, as said, combines a legal and a criminological analysis of cyber VAT fraud within the European Union.

The comparative law study focused on **mapping and providing an overview of the current state of implementation of the PIF Directive (Directive (EU) 2017/1371) and Directive (EU) 2020/284 into the national legal systems of the 27 EU Member States**. Special attention was given to the legal framework applicable to VAT fraud and its cyber dimension, including sanctions and liability schemes, procedural tools available to law enforcement authorities, and the use of ICT in national anti-fraud strategies.

The criminological analysis, instead, aimed to **investigate the empirical and operational dynamics of cyber VAT fraud**, focusing on **offender behaviours**, the **enabling role of digital technologies**, and the structure of criminal schemes. A script analysis methodology was adopted to break down VAT fraud schemes—particularly carousel fraud—into sequential actions and roles, providing insights into the organisation and execution of such crimes.

The methodology combined desk research, literature review, and the involvement of a **shared network of national experts (researchers) and institutional stakeholders**, that contributed to both analyses, ensuring coherence in data collection and complementarity in the findings.

National experts from EU Member States that participated in the project

AT	Austria	Prof. Dr. Stefan Schumann
BE	Belgium	Prof. Vanessa Franssen, Ana Laura Claes
BG	Bulgaria	Prof. Dr. Savina Mihaylova-Goleminova
CY	Cyprus	Alexis Tsielepis, Nicholas Shiakalis
CZ	Czech Republic	Prof. Hana Zídková, Ondrej Malek
DE	Germany	Prof. Dr. Jens Bülte
DK	Denmark	Jacob Ravn
EE	Estonia	CSSC
ES	Spain	Prof. María Ángeles Fuentes Loureiro
FI	Finland	<i>Not want to be mentioned</i>
FR	France	Dr. Marius-Cristian Frunza
GR	Greece	Prof. Savvadou Katerina
HU	Hungary	Prof. Zsolt Szatmari
HR	Croatia	Dr. Ksenija Cipek
IE	Ireland	Prof. Paul McCutcheon, Dr. Alex Casey
IT	Italy	CSSC, Hans Roderich Blattner, Viviana Nicolella
LT	Lithuania	Prof. Gintaras Švedas
LU	Luxembourg	Dr. Loquet Erwan
LV	Latvia	Ilze Znotina
MT	Malta	Dr. Attard Robert
NL	The Netherlands	Dr. Pim Geelhoed
PL	Poland	Prof. Dr. habil. Artur Mudrecki, Prof. Dr. habil. Monika Augustyniak
PT	Portugal	Prof. Susana Aires de Sousa
RO	Romania	Dr. Ene Marilena
SK	Slovakia	Prof. Ing. Kubicová
SI	Slovenia	CSSC
SE	Sweden	Prof. Kristoffersson Eleonor

Stakeholders involved in the project as members of the Stakeholders Advisory Group (SAG)

AT	Austria	Dr. Hubert Cottogni, Former Director of the European Investment Bank Group
BE	Belgium	Dr. Raphaël Van de Sande, Customs and Excise Expert, Trainer at HEC Liège, and Researcher at the University of Liège
BG	Bulgaria	Dr. Atanas Rusev, Director, Security Program, CSD – Center for the Study of Democracy
IT	Italy	Hans Roderich Blattner, Public Prosecutor, Ministry of Justice

IT	Italy	Viviana Nicolella, Guardia di Finanza, Ministry of Economy and Finance
IT	Italy	Prof. Barbara Vettori, Council of Europe's consultant in the field of economic and organised crime, Associate Professor of criminology, University of Naples Federico II
/	International	Giuseppina Maddaluno, Programme Officer, Training and Advanced Education Unit, UNICRI – United Nations Interregional Crime and Justice Research Institute

As far as the **comparative study** is concerned, the methodology combined secondary research, legal literature review and the use of a short, concise and structured **questionnaire** designed by the research team. The **objectives of the EU CYBER VAT questionnaire** were to: i) present the status of the transposition of Directive (EU) 2017/1371 of the European Parliament and of the Council of July 5, 2017 on the fight against fraud to the Union's financial interests by means of criminal law (hereinafter "PIF Directive") into the national law of the Member States and the mapping of the national legislation of the Member States in relation to the criminal offences of VAT fraud and cyber VAT fraud; ii) identify which investigative tools/measures are used in the EU Member States to investigate and prosecute VAT fraud and cyber VAT fraud; iii) examine the role of ICT in the strategy/policy to combat cyber VAT fraud; iv) assess the legal framework for cyber-VAT fraud (e.g. MTIC) affecting the EU's financial interests in the context of e-commerce; and v) identify trends in (new) cybercriminal activities against the EU's financial interests by describing clusters of modus operandi and cyber VAT fraudsters in the EU based on case studies.

The questionnaire was distributed to national experts—mostly academics, and in some cases practitioners—who provided detailed responses for 25 Member States. For Estonia and Slovenia, desk-based research was carried out by the CSSC's research team, using secondary sources due to the absence of completed questionnaires.

As for the **criminological analysis**, the methodology combined desk research, literature review and **case study analysis**. A *corpus* of 14 case studies (12 judicial, 2 investigative) involving VAT fraud with a digital component was collected, through preliminary keyword search of the media, online press, judgment database and contributions from the established network of national experts (researchers) and institutional stakeholders. To further enrich the results, the cases were discussed during the two online focus groups conducted. A detailed description of the methodology used will be provided in Section 2.2.

Thus, the use of the same group of experts for both the legal and criminological analyses allowed for methodological alignment and a richer, cross-cutting interpretation of findings.

The **preliminary results** were communicated to the **entire established network** (consisting of national experts, researchers and practitioners as well as relevant stakeholders) and discussed in two online events. In fact, the project also aimed to activate **networks among academics** dealing with the protection of the EU's financial interests, with a focus on digitalization, and to facilitate contacts and dialogue with **institutional actors, law enforcement officials and national prosecutors**. For this reason, national experts and other relevant stakeholders (police officers and prosecutors) were invited to participate online in two focus groups.

The first focus group explored possible criminal law, criminal procedure, and other substantive legal strategies that could be implemented at the EU Member State level to effectively combat

cyber VAT fraud within the EU and the second focus group addressed the issue of cyber-VAT fraud in e-commerce.

The results of the questionnaires, along with posthumous contributions from national experts, insights gathered during the online focus groups with experts and relevant stakeholders, and the comments on the focus group minutes, have all contributed to the development of the criminological analysis and the comparative study.

Upon completion of both analyses and the drafting of the preliminary policy recommendations, **all results were circulated among the participating experts and institutional stakeholders for final review.**

Feedback was collected through written comments; this final consultation phase served to validate the content and to refine the final **set of policy recommendations** included in the present report.

2. Cyber-VAT fraud in the European Union: an empirical criminological analysis and the role of technologies

2.1 Objective and aim

The **aim** of the criminological analysis is to **examine cyber-VAT fraud** (i.e. the digital dimension of VAT fraud) in the European Union through an empirical criminological lens. Starting from the **modus operandi as well as the characteristics of the perpetrators**, this work analyses how the **Internet affects the different activities and phases that characterize the commission of the crime of VAT fraud in the European Union**. The activity was carried out as part of WP2 “Cyber-VAT fraud: comparative criminological and criminal law analysis” of the EU-funded project “EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study”. The project is conducted by the Centre for Security and Crime Sciences (“CSSC”) of the University of Trento and the University of Verona with the financial support of the Directorate General for the European Anti-Fraud Office – OLAF Union Anti-Fraud Programme – EUAF. For more information on the objectives of the project, please see the box below.

As there is currently no effective and uniform definition of cyber VAT fraud, we have developed the following phenomenological definition of cyber VAT fraud to guide our analysis:

Cyber VAT fraud involves the use of technology to facilitate the criminal activity as a whole or to assist in one or more of its stages/phases. The use of technology at one or more stages/phases may include the creation of shell companies using forged documents or identities, the conduct of online transactions and the sale of online goods, including digital goods.

By ‘cyber VAT fraud’, the authors mean VAT fraud **facilitated by new digital technologies/elements**, as is the case in many digital organized crime activities (Di Nicola, 2022). **Digital facilitation can take place at various stages** (e.g. at the financial transaction stage, where money flows can be facilitated through online transactions); **through specific activities** (e.g. hacking to steal documents/information, creating fake documents or setting up fake companies through online channels/tools); **or through the creation of new digitally generated intangible technologies** (e.g. cloud service, software, carbon credits).

The research team, supported by institutional actors, national experts (one per Member State) and relevant stakeholders, adopted a multidisciplinary and integrated approach to assess the behaviours realised in cyberspace that could harm the EU's financial interests by evading VAT, with the aim of understanding the objective and subjective dimensions of cyber VAT fraud in the EU - the modus operandi and characteristics of the actors - with a particular focus on how digital technology is misused to commit these crimes.

The **specific aims** of the present analysis are:

- a) to outline the **modus operandi** through the formation of **behavioural clusters**;
- b) to outline the **characteristics of cyber VAT fraudsters** in the EU through the formation of **actors' clusters**;

- c) to gain a better understanding of the **role of ICT in the commission of cyber VAT fraud** (e.g. falsification of tax documents and the creation of "fake virtual companies" used for non-existent businesses).

2.2 Research design and methods

To achieve the above-mentioned aims, a **qualitative methodology** was used to analyse the *modus operandi* of cyber VAT fraud and, in particular, a **crime script analysis** was used to distinguish the **different stages and activities** in the commission of VAT fraud and to clarify the **use of ICT in the commission of VAT fraud**. The data was extracted from **14 case studies** and **2 focus groups**, as explained in more detail below.

The **script approach** has had great success in criminological research as it sheds light on the *modus operandi* of offenders in committing a particular criminal activity by focusing on identifying specific criminal opportunities and explaining how they are exploited (Lavorgna, 2014). The concept of 'crime scripts' was developed by Cornish (1994) **to describe the key stages of criminal activity** and to make the decision points clearer.

For example, script analysis has mainly been used in the study of predatory crimes such as sexual crimes against women and children, robbery and theft (et al: Tremblay et al, 2001; Petrosino and Brenisilber, 2003; Smith, 2005; Chiu & Leclerc, 2017; Chopin & Beauregard, 2020; van der Bruggen et al, 2021) and in cases of check and credit card fraud (Mativat and Tremblay, 1997; Lacoste and Tremblay, 2003), employee cybercrime (Willison, 2006), migrant smuggling (Sarrica, 2005), antiquities trafficking (Weirich, 2019), wildlife trafficking (Lavorgna, 2014), terrorism offenses (Clarke and Newman, 2006), and money laundering (Morselli and Roy, 2008; Gilmour, 2014).

Various authors have used this approach to study organized crime (including: Morgenthaler & Leclerc, 2023; Chainey & Berbotto 2022; Hancock & Laycock, 2010; Chiu et al, 2011; Tompson & Chainey, 2011; Savona, 2010), as recommended in particular by Cornish and Clarke (2002).

Some authors have specifically addressed financial crime scripting by adding financial components to the crime scripting method, arguing that it provides valuable insights for analysing all forms of for-profit crime (Snaphaan & van Ruitenburg, 2024).

Few authors have examined emerging Internet-facilitated fraud using a crime script approach (Leclerc & Morgenthaler, 2023), and of the few that have specifically examined fraud facilitated by the Internet, no work was found that uses a crime script approach to analyse VAT fraud and cyber VAT fraud.

For this reason, the authors have chosen to apply this methodology to VAT fraud as it provides an effective framework for **understanding all stages of the process of committing crime** (Van Nguyen, 2022) and for understanding **how and where (at what activity/stage) the internet has facilitated this type of fraud**. Indeed, in the context of fraud, this approach provides valuable insights into the operational knowledge of perpetrators that can contribute to the **disruption of fraudulent activities**, whether they are carried out online or offline (Leclerc & Morgenthaler, 2023). In order to understand the phenomenon and to identify the criminal activities with which this type of fraud is committed, as well as to understand how *modi operandi* have changed with digitalisation, it is essential to examine **case studies**.

Indeed, this work draws on **two data collection strategies** (Hagan, 2011), namely **case studies of VAT fraud offences** (particularly court cases) where the use of the Internet played an important

role, and **two online focus groups** with selected national researchers/experts and relevant stakeholders.

In terms of **sources and case selection**, relevant case studies were initially identified through a preliminary keyword search of the media, online press and online judgment database. Further cases from the different EU countries were collected through institutional contacts, in particular with authorities and officials actively involved in the fight against cyber VAT fraud (e.g. the Italian Guardia di Finanza), as well as through the national researchers involved in the project (one per Member State). A purposive sample was drawn to select the cases to be included in the analysis. Only VAT fraud that concerned Member States of the European Union and in which the Internet played a "significant" role were included. More specifically the **criteria for inclusion** in the investigation were therefore: 1) a case of VAT fraud affecting the financial interests of the EU; 2) a case of VAT fraud involving at least one cyber element; 3) the source contained details of the cyber elements of the VAT fraud and of the behaviors of the perpetrators.

On the basis of these criteria, **12 court cases** (CC) were selected for analysis, namely 2 Italian (CC01, CC02), 3 Spanish (CC03, CC04, CC05), 3 Dutch (CC06, CC07, CC08) 1 Lithuanian (CC09), 1 Polish (CC10), 1 Czech (CC11) and 1 Belgian (CC12).

Other national experts for the remaining Member States (e.g. Greece) have pointed us to the official annual reports of the national prosecution authorities as a source of more emblematic cases.

Given the difficulty of covering all states and to find judicial cases, we also tried to extrapolate cases from the official reports of each national police authority, which we refer to as investigative cases (IC), but which we wanted to distinguish from the other court cases collected, as in many cases investigations are ongoing and we do not have the normative references.

In particular, as they met the inclusion criteria, we selected an investigative case for Greece (IC01) described in the annual reports of the Financial Police Directorate (2023) and an investigative case reported in the annual report of the EPPO (2023) that mainly concerned Spain, but the network also involved other EU and non-EU countries (IC02), so we included a total of **2 investigative cases**.

This brings the total number of cases considered to 14.

For the other countries, the national experts either did not provide us with cases (Denmark, Cyprus, Finland, France, Germany, Luxembourg and Slovakia) that met our inclusion criteria, or in many cases they provided us with newspaper articles (reporting on known cases, e.g. the Admiral case) that did not provide enough details on the modus operandi and the role of digitization (e.g. Malta) and for which no further material could be collected as they were not yet closed.

It should be noted that the publicly available case law on VAT fraud is quite limited, especially in relation to cases of fraud enabled and/or facilitated by technology. It was therefore difficult even for the national researchers involved to find suitable examples that met our research needs.

Searching for cases on the online pages of traditional newspapers and financial newspapers as well as online websites in the hope of finding articles on cases of VAT fraud also revealed descriptions of new cases, but with very limited information, particularly in relation to the digital element. Even when reviewing EPPO press releases and relevant parliamentary questions on VAT fraud, there were few findings on cyber VAT fraud.

Once the cases were identified, **cyber VAT fraud was broken down into key stages** for investigation. This was done to determine **when and how the Internet is used**. To this end, the data was analysed using a script model based on the work of Hancock and Laycock (2010) and Lavorgna (2013). Moving on to the actual script of a carousel fraud, as in Lavorgna's model "The Crime Script for

Identifying Internet-Related Criminal Opportunities” (2013), the main stages have been identified, including the stages that precede and follow the actual scam. The **ten stages** are as follows:

- Stage 1: Preparatory activities that precede the commission of the carousel fraud;
- Stage 2: Creation/opening of the “missing trader” to commit the fraud;
- Stage 3: Initial sale: intra-EU VAT-free transaction (A → B);
- Stage 4 (eventual): Multiple resales (B → Buffer(s) → C);
- Stage 5: Internal sale with VAT (B → C);
- Stage 6: Non-remitting of the collected VAT (by B);
- Stage 7: Disappearance of company B (becoming missing trader) as an exit strategy (activity to evade the authorities);
- Stage 8: Final sale: intra-EU sales without VAT returned to the first seller (C → A);
- Stage 9: Request for refund of VAT paid (by C to B, missing trader);
- Stage 10: Post-fraud activities directly resulting from or following the fraud.

The **single actions performed by the fraud actors** at each stage were identified in a general “Action” column (see Table 2), and each action was assigned a **function** using the “sequence of functions in the crime scene” identified by Cornish (1994) and described by Hancock and Laycock (2010), namely: preparation, entry, precondition, instrumental initiation, instrumental actualization, action, postcondition, and exit. Indeed, as shown in the table 2, from Hancock and Laycock ‘s (2010) “integrated organized crime script” model, the labels “function” and “action” were retained and a specific column “Action in which the Internet was used” was added, as in Lavorgna’s model (2013).

2.3 The analysis

Clusters of *modus operandi* and actors

Firstly the **modus operandi** and the **actors involved in cyber VAT fraud** have been examined, through a detailed analysis of the selected cases.

The **ten stages** identified in the previous section represent the **course of action** we found in the VAT fraud cases we investigated, which consists of a series of behaviours aimed at planning (before), carrying out and protecting (after) a specific criminal act in order to avoid detection. The individual activities and the impact of digitalisation on them are examined in the next section.

The starting point was the identification of the main VAT fraud schemes known in the literature and the classification of those found in the case studies examined.

Traditional VAT fraud can be divided into two broad basic categories according to a classification based on the **type of scheme**, depending on whether the ill-gotten gain consists of a **reduction in the tax due** (tax evasion) or **VAT misappropriation** (non-payment of VAT due and/or false claiming of tax credits), or both (Fedeli & Forte, 2011). A further classification can be made based on the complexity of the fraud scheme: whether the fraud involves only a domestic or an international (intra-community) component, a single transaction or a chain of “carousel transactions” and how complex the carousel is (Fedeli & Forte, 2011).

As mentioned above, the most common form of VAT fraud is the so-called **MTIC (Missing Trader Intra-Community) fraud**, and an important form of MTIC fraud is **carousel fraud** (CEPOL, 2022), which is also the pattern of VAT fraud we found in our case studies (see Table 1). The following schemes can be distinguished in detail:

- **MTIC acquisition fraud** (the simplest type of MTIC fraud): company A (supplier or seller) in Member State 1 sells goods or services to company B (missing trader) in Member State 2. As this is a cross-border transaction, the zero rate applies. Company B then sells the goods or services to company C (broker) in Member State 2 and the VAT rate of Member State 2 applies. After the sale, company B disappears without paying the VAT due to the tax authorities of Member State 2 (European Parliament, 2021);
- **MTIC carousel fraud (“closed carousel”)**: company A (supplier or "conduit" company) in Member State 1 sells goods or services to company B (missing trader) in Member State 2. In this case, the zero rate for VAT applies. Company B sells the goods and services to company C (broker) in Member State 2 and the VAT rate of Member State 2 applies. Company B then disappears without remitting the VAT due. Company C then sells the goods or services back to company A in Member State 1. Since company C bought the goods on the domestic market of Member State 2, it had to pay the VAT to company B (European Parliament, 2021);
- **MTIC carousel fraud (“open carousel”)**: it is the same scheme as the closed carousel, with the difference that company C (broker) resells the goods to other companies operating in its country or directly to the final consumer (domestic VAT-taxable supply), deducting the VAT previously paid to company B (missing trader).

As already mentioned in the introduction, in both forms of carousel fraud, one or more buffer companies may be interposed between the missing trader (B) and company C in order to conceal the fraud from the authorities and extend the chain of fraud.

The following is an **example case description of the type of scheme** we found in each of the case studies analysed (see Table 1).

Table 1 – Type of scheme in selected case studies

Cases	Modus operandi
CC01, CC02, CC04, CC05, CC09 IC01	Misappropriation of VAT MTIC carousel fraud with a complex chain of paper companies and buffers
CC03, CC12	Reduction of the tax due Misappropriation of VAT MTIC carousel fraud with a complex chain of paper companies and buffers
CC06, CC07, CC08, CC10 IC02	Misappropriation of VAT MTIC carousel fraud with a complex chain of paper companies and buffers (also involving non-EU states)

Despite the geographical and contextual diversity of the cases, several similarities emerged in the fraudulent behaviour and characteristics of the perpetrators. These common patterns highlight the structured nature of VAT fraud and the sophisticated exploitation of systemic and technological vulnerabilities across borders. We have identified the following clusters of criminal behaviours and actor characteristics. By clustering actions and identifying roles, the analysis provides a comprehensive understanding of the strategies used by fraudsters and the interplay of actors within these schemes.

Common aspects in modus operandi - clusters of behaviours:

- *Formation of shell companies: fraudsters set up or acquire dormant companies and use false identities and documents to carry out transactions that exist only on paper;*
- *Chain transactions: setting up complex networks of "missing trader" companies, which are often young and have no significant operational history or physical presence, and "buffer" companies to disguise the fraudulent activities. Buffer companies are used to extend the transaction chain, making it more difficult to detect the fraud scheme⁸;*
- *Fictitious transactions: no real movement of goods between buyers and sellers (non-existent transactions);*
- *Falsification or manipulation of documents: use of false declarations, forged invoices and documents to feign legitimate sales and purchases;*
- *Exploitation of EU VAT rules: exploiting the rules for tax-free intra-Community supplies;*
- *Digital facilitation: the Internet is used as a tool for many activities (e.g. payments);*
- *Profit distribution: smuggling of fraudulent profits via offshore accounts or reinvestment in legitimate businesses to disguise the origin of the funds.*

Common characteristics of cyber VAT fraudsters - clusters of actors:

- *Organised groups: typically, the fraud involves individuals belonging to structured criminal organisations with different roles.*
- *Professional expertise: in other cases, the organisers are high-level individuals who hold the position of president and/or vice president of large companies and coordinate the entire fraud scheme. The "coordinators" of the fraud are individuals with expertise and professional background in tax law, financial operations, tax regulations and digital tools who join forces with each other (in the form of organised groups) to commit one or more tax crimes or with the specific aim of committing VAT fraud⁹.*

⁸ For example, in the Polish case - Judgment No. 466/2020 (C10) - a network of 10 interconnected entities (many of them fictitious companies) was set up to simulate a trade in hosting services. A single individual ran the network and registered and managed the domains of the entities, which had websites designed to create an appearance of legitimacy.

⁹ For example, in one of the Italian cases investigated (CC01) - Criminal judgement § 3 no. 24258/2023 - the defendants were the chairman of the board of directors, the deputy chairman and the person responsible for purchases and sales, who issued and used invoices for non-existent transactions in mutual agreement to circumvent so-called intra-Community VAT in the area of IT products (such as Microsoft Office packages).

- *Large network of accomplices: this is a network of accomplices, including fake directors ("fronts") who act as administrators for shell companies and other intermediaries that facilitate the transfer of funds and goods.*

In relation to the authors, **three levels of participation** can be summarised as follows (Aronowitz et al., 2004):

1. **Core organisers (level 1):** these inner circle actors plan and execute the fraud, often avoiding direct connection with the companies involved, although they receive the largest share of the profits.
2. **Outer circle actors (level 2):** this group includes “straw men” (dummy managers), accountants, lawyers, IT specialists and other professionals who facilitate the fraud by creating fake documents or providing technical support (Middleton & Levi, 2004).
3. **Facilitators (level 3):** Legitimate businesses, such as “buffer companies”, unwittingly participate by processing VAT-exempt goods or accepting fraudulent invoices (Borselli, 2011).

At the first level, the people behind the creation or purchase of the missing trader are usually the actual organisers of the fraud. In some cases¹⁰, in addition to the organisers, there were **operational managers** in the inner circle who ran the day-to-day operations, including preparing transactions, managing shell and filter companies, and overseeing logistics.

The organisers are usually individuals belonging to **criminal organisations** dedicated to other types of crime and using VAT fraud for capital laundering, or criminal organisations operating across borders through companies operating in several Member States (EPPO, 2023) and exploiting the VAT system for large-scale fraud. In fact, criminal organisations (especially mafia-type organisations) are becoming increasingly entrepreneurial and hide in the social fabric by penetrating the economic-productive system and intercepting the flow of funds (from individual states and the European Union) for public works or to support families and businesses. Nowadays, criminal organisations manage to obtain the necessary financial resources by using the most advanced techniques of money laundering, tax evasion and fraud and/or by creating illicit funds through VAT fraud ("carousel fraud") (Villani, 2023). In addition, the EPPO's annual report (2022) confirms the claim that organised crime groups finance VAT fraud operations with capital derived from their other illegal activities. There are also individuals and entities engaged in money laundering that facilitate the conversion of funds from VAT fraud and other criminal activities of these groups (EPPO, 2023)

However, at the second level, we find "front men" who were often unaware of the full extent of the fraud but played a role in lending legitimacy to the fraudulent entities, and individuals with **specialised roles**, such as professional accountants, tax advisors and IT specialists¹¹, play a crucial role, especially as the rise of **Crime-as-a-Service (CaaS)** allows fraudsters to outsource digital expertise. For example, phishing attacks can be used to steal company data to set up bogus companies (Kothakonda et al., 2004).

Although the cases investigated had many similarities, they differed in scope and complexity. The Italian case, for example, showed a higher level of logistical sophistication and hierarchies (adopting a more 'traditional' guise of VAT fraud), while other cases showed greater sophistication

¹⁰ e.g. Italian Case (CC01) - Criminal judgement § 3 no. 24258/2023

¹¹ For example, in one Dutch case (CC07) - Rechtbank Overijssel (Nederland) No. 08/993150-19 (P) (FP) 2021 - there was a person specifically designated as “responsible for the of computerisation”.

in terms of the use of technology for both digital manipulation and online purchase of services (online purchase of defunct companies to convert them into paper mills¹².

In the next section, we will take a closer look at the aspects related to the use of technology and the criminal possibilities of digitalization and how these affect the different stages of VAT fraud.

The role of ICTs: script analysis and interpretation

As seen, one of the recurring aspects in the cases analyzed was the “digital facilitation”, where the Internet is used as a facilitator in different activities/stages of the commission of VAT fraud.

The majority of the cases analyzed primarily **involved simulated transactions** — i.e. **objectively non-existent operations**¹³ — facilitated by trading in **digital goods** (e.g. hosting services¹⁴, Microsoft Office packages¹⁵). The goods concerned – which are always among the goods with a high risk of VAT fraud, such as technical equipment and digital goods (cloud storage and software) – were only transferred at an accounting level, without any physical movement taking place. This was achieved through the use of simulated transactions and falsified documentation, such as fake invoices. The advent of **intangible digital goods** has made it easier to carry out such fraudulent activities. These goods can be transferred almost instantly, are more difficult to trace and do not require the same logistical infrastructure as physical goods (Masca, 2022). In the past, VAT fraud often involved low-value items (e.g. cell phones, computer chips, microprocessors, hi-fi equipment, new or used vehicles or precious metals, memory cards). However, with the increasing digitalization of VAT fraud, intangible products are becoming more common, especially in carousel fraud. These products can change hands across borders in a matter of minutes and the entire fraud process can be completed very quickly. Furthermore, as no physical logistics or document monitoring (e.g. warehouse or transportation documents) is required, these frauds are much easier to carry out.

In the selected cases, “paper” companies were repeatedly set up with the aim of committing fraud or purchased on internet platforms: As mentioned above, in some cases, dormant companies with a broad corporate purpose, which were then converted into paper mills, were bought on websites offering dormant or “silent” companies for sale, even with a “straw man” person as their administrator¹⁶.

The specialised literature also mentions the possibility of setting up “virtual companies” (Directorate of Financial Police - Annual Reports 2023, Hellenic Police) by acquiring (e.g. on the Dark Net) stolen tax data and credentials of real companies and impersonating them in order to carry out so-called **subjectively non-existent transactions**. However, we did not encounter these activities in our sample of case studies.

¹² Spanish case (CC04) - Supreme Court, Criminal Section, Judgment No. 675/2019.

¹³ “Objectively non-existent” are called those transactions characterized by the partial or total absence of the invoiced supply or service; thus, services are invoiced that were never actually performed.

¹⁴ Polish case (CC10) - Provincial Administrative Court in Poznań, Judgment No. 466/20.

¹⁵ Italian case (CC02) - Supreme Court, Judgment No. 24257/2023

¹⁶ Spanish case (CC04) - Supreme Court, Judgment No. 675/2019. In this case study, one of the defendants was being convicted of putting up for sale through the Internet inactive “dormant” companies, ready to be used in the fraud, and also a “front man” to be placed as their administrator through his website (www.sociedadesurgentes.com).

In addition, in some cases, undeclared accounting software was used to track real and fictitious transactions and manage "parallel markets" via separate digital registers¹⁷.

In almost all cases, digitalization appears to have had a particular impact on the facilitation of banking transactions. Numerous bank accounts were often used and countless debit cards were managed via online banking and digital access data (codes, passwords)¹⁸. By exploiting home banking in particular, fraudsters were able to open and close bank accounts with great ease and speed in order to carry out fraudulent transactions while bypassing controls¹⁹.

Finally, in all the cases analysed, we found the creation (and use) of false documents (e.g., fake invoices) and/or the manipulation of existing documents (e.g., falsifying tax returns): the goal is to create false evidence of one or more transactions in order to commit so-called objectively nonexistent transactions. It is obvious that the current digital environment has created a favorable environment for tax fraudsters to use document forgery and manipulation technologies, but unfortunately we did not find specific details on digital manipulation/falsification techniques in the various documents related to the cases analyzed.

Based on these findings, and in view of the stages described above, the data have been compiled in the following table (Table 2), highlighting for each activity of the fraudsters use of ICTs.

It must be specified that this script framework does not include all the actions required to commit VAT carousel fraud but focuses on those where the Internet was used, as found in the case studies examined. Thus, in the Table, for each stage of VAT fraud (as described in the case studies analyzed), the reader will find the various functions in the activity and the corresponding actions, as well as the type of Internet use in that specific action.

In particular, the script for cyber VAT fraud outlines a **series of actions in which the Internet acted as a facilitator**. The Table (column *Action in which ICTs are used* in Table 2) shows how the possibilities of the internet are exploited, both for services (e.g. e-mail providers and instant messaging) and for online "places" (e.g. certain commercial websites) where the services needed to commit fraud can be purchased.

In the selected cases, several companies (buffers) based in different countries (sometimes even outside the EU) were always involved. However, as already explained, the use of filter companies (buffers) is not necessary for the commission of fraud, although in the analyzed cases often buffers were interposed to further complicate the tracing of the trade; for this reason, the function of this action has been referred to as 'eventual' (see Table 2).

Using this conceptual framework, it was possible to identify **five main types of criminal facilitation/opportunity that the Internet and digital society provide for the commission of this crime**, namely:

¹⁷ Spanish case (CC03) - Supreme Court, Judgment No. 40/2020. In this case study, all these purchases (both domestic purchases and purchases to other European MS) were made by the trading department in parallel accounting records, which the company itself called 'special control', managed by the Director of the Trading Department who was responsible for 'special control'.

¹⁸ e.g. Dutch case (CC08) - Amsterdam Court of Appeal, Case Number 23-001665-21, year 2023. In this case study, the defendant used a large number of bank accounts, with 84 debit cards and digital access data (codes, passwords) found in his possession.

¹⁹ Dutch case (CC07) - Overijssel District Court, Case Number 08/993150-19 (P) (FP), year 2021.

1. Communicative facilitations/opportunities: communication with suppliers and customers is facilitated by the use of services such as e-mail and Skype;
2. Organizational facilitations/opportunities: the use of the Internet facilitates the internal organization of the parties and (if any) the criminal network. The Internet eliminates the need for direct contacts with the actors involved in cross-border trade or with the end users and facilitates contacts between them;
3. Information facilitations/opportunities: the Internet makes it possible to access useful information and find out about certain online services that can provide solutions to specific problems. For example, the ability to obtain information about a company (e.g. VAT numbers) or to buy inactive companies to use as missing traders;
4. Economic facilitations/opportunities: transferring funds between bank accounts is done digitally, via online banking systems and using instant transfers, so money can be moved faster;
5. Logistical facilitations/opportunities: high-risk goods and digital goods are used, which can be easily moved using only accounting and simulated transactions, without the need for transportation documents or warehouses.

Table 2 - The crime script for Cyber VAT fraud in the European Union

Stage	Function	Action	Action in which ICTs are used
1	Instrumental Initiation	Identify and mapping existing service for purchasing inactive companies or identify how to quickly open a new company	Web research
1	Preparation	Formation / existence of the criminal network with other party	Online contacts (email, skype)
1	Instrumental Initiation	Recruitment of professionals (e.g. accountants, tax advisors and lawyers and IT specialists)	Online contacts (website, emails)
1	Preparation	Establishing contacts with suppliers and customers	Online contacts (online trading websites, emails, Skype)
2	Instrumental Initiation	Creation of a fictitious company B (missing trader)	Buying inactive companies via certain websites, together with a "straw man" who is used as their administrator to exploit them for fraud
2, 3, 4 and 5	Precondition	Maintenance of contacts with other party	Online contacts

Stage	Function	Action	Action in which ICTs are used
			(email, skype)
3	Instrumental actualization	Initial sale VAT-free (A → B)	Buying and selling in e-commerce. Buying and selling can involve digital (intangible) goods.
3	Doing	Invoicing initial sale (A → B)	Use of e-invoicing. Creation of false invoices (Internet)
3	Doing	Creation of fake documentation related to initial sale (A → B)	False purchase and sales contracts, false purchase orders and other documents with false information on transactions and business partners created using technology
4	Eventual	Multiple Resales (B → Buffer(s) → C)	Payments by express bank transfer or instant bank transfer with online banking
5	Instrumental actualization	Internal sale VAT-inclusive (B → C)	Buying and selling can take place in e-commerce. Buying and selling can involve digital (intangible) goods.
5	Doing	Invoicing internal sale (B → C)	Use of e-invoicing. Creation of false invoices (Internet)
5	Doing	Creation of fake documentation related to internal sale (B → C)	False purchase and sale agreements, false purchase orders and other documents containing false information about transactions and business partners created with the help of technology
6	Doing	B non-remitting the collected VAT	Omitting VAT declarations online
8	Instrumental actualization	Final sale VAT-Free to initial seller (C → A)	Buying and selling can take place in e-commerce. Buying and selling can involve digital (intangible) goods.
9	Instrumental actualization	C VAT Refund Claims	Use of e-invoicing for automatic claim

Stage	Function	Action	Action in which ICTs are used
7	Exit	Disappearance of Missing Trader (B)	Fast closing through access to online platforms for company registration and by completing the closing forms directly online
10	Postcondition	Dividing the proceeds of VAT fraud among all actors	Faster and anonymous economic transactions (cryptocurrency, blockchains) on accounts abroad

2.4 Concluding remarks

This criminological analysis highlights the **significant and multi-layered impact of digitalisation on VAT fraud in the European Union** and provides a comprehensive understanding of **how the internet and related technologies facilitate the commission of these crimes**. By applying the script analysis method to the collected case studies, this study systematically breaks down the stages of cyber VAT fraud and sheds light on the operational techniques used by the perpetrators and the criminal opportunities offered by digitalisation.

One of the **key findings** of this study is that the **internet plays a central role in every stage of VAT fraud, from the preparatory stages to the post-fraud activities**. Digital tools and platforms streamline critical processes such as communication, the acquisition of shell companies, the falsification of documents and the execution of financial transactions.

In particular, it has been found that perpetrators often use online platforms to acquire dormant companies, usually run by straw men as administrators. These companies are sold so that they can be used as "paper companies" for fraudulent schemes. This phenomenon represents a form of industrialisation of cybercrime, where specialized individuals or organized groups create "products" (e.g. ransomware) to be sold. This practice falls under the broader concept of "Crime-as-a-Service" (CaaS), where individuals or criminal organizations that do not have the technical expertise or resources to develop specific tools (e.g. viruses or fraudulent software) can instead purchase them to carry out criminal activity more efficiently. In our case, these dormant companies were purchased and then used as "missing traders" to disguise illegal activity and evade tax liabilities.

In addition, the creation of forged documents, such as invoices and purchase orders, is further facilitated by digital tools, while instant online banking enables fast financial transfers across national borders, making it more difficult to trace and intercept fraudulent transactions.

The study also shows how digitalisation has increased the scale and complexity of VAT fraud. Unlike traditional fraud methods, **cyber VAT fraud takes advantage of the dematerialisation of assets and transactions**, reducing the need for physical goods or infrastructure. The increasing prevalence of intangible assets such as digital services and software has made it easier for perpetrators to orchestrate fraudulent activity without the physical movement of goods, relying instead on simulated transactions. This evolution in fraud methodology poses particular challenges for law enforcement agencies, as digital goods and services are more difficult to track.

In addition, the analysis confirms that **organized crime groups play an important role in VAT fraud, often supported by networks of professionals such as accountants, IT specialists and tax advisors.** These actors use their expertise to exploit weaknesses in the system and design sophisticated fraud schemes that circumvent detection mechanisms.

This analysis is an important step towards developing more effective strategies to combat VAT fraud as it sheds light on the phenomenon and its current manifestations. It highlights the importance of understanding the intersection between technology and crime and predicting how future advances in digitalization may further impact criminal opportunities.

Several key actions are needed to address these challenges. First, as the findings suggest that **large networks of companies in multiple Member States (and sometimes even non-EU countries) are involved**, there is an urgent need to strengthen international cooperation between Member States to ensure continuous information sharing and coordination of enforcement actions. Secondly, given the advanced nature of technology, **investment in technological expertise is essential to equip control authorities with the necessary tools and knowledge to detect and expose sophisticated VAT fraud schemes.** Thirdly, given the speed at which goods and money can now move thanks to technology, the **introduction of advanced digital tools to monitor and detect fraud in real time is essential.** Together with a stronger legal framework, these tools can help close existing gaps and improve the EU's ability to respond to new threats. These aspects will be addressed in the comparative study on criminal law and criminal procedure, which will be included in the final report of the project together with this analysis.

3. Pif Directive (Directive 2017/1371/EU) and its implementation in the Member States

The European Union's efforts to secure the financial interests of its member states have been significantly strengthened by the **adoption and transposition of the PIF Directive** (Directive (EU) 2017/1371). This Directive addresses crimes affecting the Union's financial interests, particularly in the context of Value Added Tax (VAT) fraud and the emerging domain of cyber VAT fraud.

The PIF Directive was adopted to replace the 1995 Convention on the protection of the EU's financial interests. It extends the scope of criminal liability, introduces harmonized definitions for offenses such as VAT fraud exceeding €10 million, and sets minimum penalties.

This paragraph of the Final Report will revisit the legal analysis concerning the implementation of the Directive across the various Member States, with particular focus on its most significant provisions: notably, Article 3 (concerning VAT fraud committed by natural persons), Article 7 (sanctions on natural persons), Article 6 (liability of legal persons), and Article 9 (sanctions on legal persons).

To do this, these topics were addressed in the questionnaire submitted to the national experts. In the questionnaire, about compliance with Article 3 of the PIF Directive, respondents were asked to confirm or clarify the conclusions in the first annex provided (Annex 1), which contained the results of the preliminary analysis carried out by the CSSC (Q. 1).

Article 3 of the PIF Directive requires Member States to adopt the necessary measures to punish intentional conduct that causes damage to the financial interests of the EU. It establishes what constitutes fraud under EU law in connection with revenues and expenditures, giving a list of conducts that shall be regarded as fraud. These conducts are differentiated based on whether they affect EU Revenue or EU Expenditure and they can be summarized as follows:

- fraud involving revenue refers to acts that diminish the financial interests of the EU, including misrepresentation or concealment of information related to VAT or customs duties; submission of false or incomplete statements; non-disclosure of information that leads to a reduction in EU revenues.
- fraud related to EU expenditures includes: the use or presentation of false, incorrect, or incomplete statements or documents, leading to the misappropriation or wrongful retention of EU funds; failure to disclose information, which results in the misappropriation or wrongful retention of EU funds; misapplication of funds for purposes other than those for which they were granted.

Respondents were then asked to indicate which types of VAT fraud are covered by their national law (Q. 1,1) and what **subjective intent** is required for punishment: intentional, unintentional, or both (Q. 1,2).

The study also examined the sanctions framework outlined in the PIF Directive, focusing on **penalties for natural persons** under Article 7 (Q. 2) and those for legal entities under Articles 6 (Q. 4) and 9 (Q. 5). Article 7 of PIF Directive addresses the criminal sanctions that Member States must apply to natural persons who intentionally commit offenses that harm the EU's financial

interests, ensuring these penalties are effective, proportionate, and dissuasive. Meanwhile, Articles 6 and 9 detail the obligations of Member States to ensure that **legal persons** can be held liable for such offenses, either directly or due to a lack of oversight by individuals in positions of authority. These provisions emphasize the importance of robust sanctions to deter VAT fraud and protect the EU's financial interests.

As for question n. 1, also, or questions number 2 and 4 respondents were asked to confirm or clarify the conclusions in the annexes provided (respectively *Annex 2* and *Annex 3*), which contained the results of the preliminary analysis carried out by the CSSC.

Finally, the consistency of the PIF Directive with Article 8, which addresses the **aggravating circumstances for VAT fraud in the context of organized crime**, was examined (Q. 3). There is a reference to Framework Decision 2008/841/JHA, which governs the fight against organized crime in Europe.

As previously noted, VAT fraud—and fraud in general—is the second most exploited market by criminal networks. These networks have a significant capacity to operate across Member States, posing a serious threat to the financial interests of the EU. This underscores the urgent need for an efficient and coordinated response to address this issue effectively.

Disclaimer: Not all legal translations provided are official. Some have been translated by experts, while others were prepared by the CSSC.

3.1 National legislations

Austria

As already mentioned, article 3 of the PIF Directive concerns the criminalization of the commission of fraud to the detriment of the EU's financial interests. **Austria is compliant with Article 3 of the PIF Directive.** Austria has achieved compliance by **introducing completely new legislation**. Indeed, the previous national legal provisions did not meet the minimum requirements set out by the Directive [see Federal Law Gazette 129/1958 as amended by Federal Law Gazette I 62/2019]. For this reason, the European Commission initiated an infringement procedure against Austria, which was concluded in May 2022.

Various provisions in the Fiscal Criminal Code penalize these phenomena, ranging from general tax evasion [see § 33 FinStrG²⁰] to tax fraud [§ 39 FinStrG²¹], including the article § 40 FinStrG²² that specifically regulates cross-border tax fraud.

According to the national expert, Austrian national legislation classifies VAT fraud as a general offense (**free form**), which means that no specific conduct or actions are explicitly defined. The conducts outlined by articles are very broad.

With regard to the **subjective element**, Austria provides that only **intentional acts** are punishable. Article 34 FinStrG establishes liability for the actions outlined in Article 33, even in cases of gross negligence [see § 34 on negligent tax evasion²³].

²⁰ § 33 FinStrG. Tax evasion

(1) Any person shall be guilty of tax evasion who intentionally causes a tax reduction in violation of a duty of notification, disclosure or truthfulness under tax law.

(2) Any person shall also be guilty of tax evasion who intentionally causes

a) in breach of the obligation to submit advance VAT returns in accordance with § 21 of the Value Added Tax Act 1994, a reduction of VAT (advance payments or credit notes)

[...] and considers this not only possible but certain [knowledge].

(3) A tax reduction pursuant to subsection 1 or 2 shall be deemed to have been effected [...]

²¹ § 39 FinStrG. Tax fraud

(1) Any person is guilty of tax fraud who commits the financial offences - to be punished exclusively by the court - of tax evasion, smuggling, evasion of import or export duties or tax theft pursuant to section 37 (1) by

a) using false or falsified documents, false or falsified data or other such evidence, with the exception of incorrect tax declarations, notifications, reports, records and profit calculations to be drawn up in accordance with tax, monopoly or customs regulations, or

b) using fictitious transactions or other fictitious acts (§ 23 BAO) or

c) using books or records created with the aid of automated systems and required to be kept in accordance with tax or monopoly regulations, which have been influenced by the design or use of a program with the aid of which data can be changed, deleted or suppressed

commits an offence.

(2) Any person who commits a financial offence of tax evasion to be punished by the court by claiming input tax amounts that are not based on deliveries or other services in order to affect a tax reduction without fulfilling the offence in subsection 1 shall also be guilty of tax fraud.

(3) (a) Anyone who commits tax fraud is liable to a custodial sentence of up to five years. In addition to a custodial sentence not exceeding four years, a fine of up to 1.5 million euros may be imposed. Associations are liable to an association fine of up to five million euros.

(b) Anyone who commits tax fraud with a criminal value exceeding 500,000 euros is liable to a custodial sentence of one to ten years. In addition to a prison sentence not exceeding eight years, a fine of up to 2.5 million euros may be imposed. Associations are liable to an association fine of up to eight million euros.

²² § 40 FinStrG. Cross-border value added tax fraud

(1) Any person who intentionally creates or participates in a cross-border fraud scheme in which supplies, or other services are wholly or partly executed or simulated shall be guilty of cross-border VAT fraud if they does so by

a) using or submitting false, incorrect or incomplete VAT returns or documents, or

b) concealing VAT-relevant information in breach of a legal obligation, or

c) fraudulently causes a loss of VAT by submitting correct VAT declarations, whereby VAT is not paid by the due date at the latest or VAT credits are unlawfully claimed,

and the loss of VAT in the Community territory (§1 (3) of the VAT Act 1994) amounts to at least ten million euros in total.

(2) Cross-border VAT fraud is punishable by imprisonment of between one and ten years. In addition to a prison sentence not exceeding eight years, a fine of up to EUR 2.5 million may be imposed. Legal entities are liable to a fine of up to eight million euros.

(3) The calculation of the loss of revenue shall be based on the amounts that would have been charged if the tax liability had arisen in Austria, unless the defendant proves the amount of the tax liability by means of a legally binding decision by the other Member State of the European Union responsible for levying the tax.

²³ § 34 Grossly negligent tax evasion

Austria is also compliant with the required **sanctions** for the commission of fraud, described in Art. 7 of the Directive, in particular with the required maximum penalty of at least 4 years imprisonment in cases where the fraud committed against the financial interests of the EU has led to a loss of more than 100.000 € (threshold established for the “considerable damage”). Austria meets the requirements. According to article 33 (3)a, the maximum sentence of 5 years imprisonment, but 3(b) foresees a maximum penalty of 10 years for frauds with a criminal value exceeding 500,000 euros. The same is foreseen for Cross-border value added tax fraud.

Similarly, about the liability of legal persons, Austria is compliant with Article 6 of the PIF Directive, having already adopted compliant provisions before the Directive's enactment [§ 28a²⁴ Fin StrG Verbandsverantwortlichkeitsgesetz (VbVG) Act on Liability of Legal Entities for Criminal Offences, Artt. 1, 3²⁵, 4, 12].

In particular, Austria provides for the following sanctions (as indicated by Art. 9 of the PIF):

- criminal fine (not specified);
- exclusion from entitlement to public benefits or aid [sectoral regulations];
- temporary or permanent exclusion from public tenders [§ 78(1) No. 6 Federal Procurement Law 2018, implicitly referring to tax evasion, not the offense itself];
- judicial liquidation [intrinsically with the withdrawal of the business license, § 87 GewO].

(1) Any person who commits the offence specified in section 33 (1) through gross negligence shall be guilty of grossly negligent tax evasion; section 33 (3) shall apply accordingly.

²⁴ § 28a FinStrG. Responsibility of legal entities

(1) The provisions of Sections 1 and 2 of the Act on the Liability of Legal Entities for Criminal Offences shall apply to financial offences of legal entities to be punished by the court (Section 1 (2)); however, unless otherwise stipulated in offences, the fine imposed on the legal entity shall be calculated in accordance with the fine threatened for the financial offence for which the legal entity is responsible, but under the conditions of §15 (2) [FinStrG] in accordance with 1.5 times this fine. In all other respects, the provisions of this section shall apply insofar as they are not exclusively applicable to natural persons.

(2) Sections 2, 3, 4 (1), 5, 10, 11 and 12 (2) of the Act on the Liability of Legal Entities for Criminal Offences shall apply mutatis mutandis to financial offences committed by legal entities that are to be punished by the administrative financial penal authority. The fine shall be calculated in accordance with the fine threatened for the financial offence for which the legal entity is responsible. In all other respects, the provisions of this section shall apply insofar as they are not exclusively applicable to natural persons.

²⁵ § 3 VbVG

(1) A legal entity shall be liable for an offence under the further conditions of subsection (2) or subsection (3) if

1. the offence has been committed in its favour or
2. the offence violates duties incumbent on the legal entity.

(2) The legal entity shall be liable for criminal offences committed by a decision-maker if the decision-maker as such has committed the offence unlawfully and culpably.

(3) The legal entity shall be liable for criminal offences committed by employees if

1. Employees have unlawfully committed the facts corresponding to the statutory offence; the legal entity shall only be liable for an offence that requires intentional conduct if an employee has acted intentionally; for an offence that requires negligent conduct, only if employees have failed to exercise the due care required by the circumstances; and

2. the commission of the offence was made possible or significantly facilitated by the fact that decision-makers disregarded the due and reasonable care required by the circumstances, by failing to take essential technical, organisational or personnel measures to prevent such offences.

(4) The liability of a legal entity for an offence and the criminal liability of decision-makers or employees for the same offence are not mutually exclusive.

Finally, Austrian national legislation contains an **aggravating circumstance** for VAT fraud committed in the context of **organised crime**, § 38a Fin StrG²⁶, as provided for by Article 8 of the PIF Directive.

Belgium

Belgium is compliant with Article 3 of the PIF Directive, which concerns the criminalization of the commission of fraud to the detriment of the EU's financial interests.

Belgium has achieved compliance by **amending its pre-existing legislation** after an infringement procedure was initiated by the EU Commission. The amendment was related only to the minimum sanctions because the definitions were already compliant.

Belgian national legislation classifies VAT fraud as a general offence (**free form**), which means that no specific conduct or actions are explicitly defined. The relevant legislative provisions are Articles 73²⁷ and 73 nonies²⁸ VAT Code (attempt) as last amended by L. 9 December of 2019.

With regard to the subjective element, Belgium provides that **only intentional acts** are punishable. This is explicitly provided for in Article 73 and can also be inferred from the fact that the attempt is punishable.

Belgium is, since 2019, compliant with the required **sanctions** for the commission of fraud, described in Art. 7 of the Directive, in particular compliance with the required maximum penalty of at least 4 years imprisonment in cases where the fraud committed against the financial interests of the EU has led to a loss of more than 100.000 € (threshold established for the “considerable damage”). Belgium meets the requirements and provides for a maximum sentence of 5 years imprisonment. It is necessary to underline that, in Belgium, there is a significant difference between the sanctions for “normal” VAT fraud (imprisonment of maximum 2 years, Art. 73, para. 1 VAT Code) and those for “serious VAT fraud” (imprisonment of maximum 5 years, Art. 73, para. 2 VAT Code). The latter is indeed higher than the threshold foreseen in the PIF Directive. It is worth pointing out that the PIF Directive defines the seriousness of fraud based on the damage or advantage it involves. Under Belgian law, there is no definition of what constitutes “serious fraud”.

²⁶ § 38a Fin StrG

(1) Whoever, without fulfilling the offence of § 39,

a) commits tax evasion, smuggling, evasion of import or export duties or tax theft under section 37(1) as a member of a gang of at least three persons who have joined together to commit the offense, with the assistance (section 11) of another member of the gang, [...] shall be punished in accordance with subsection 2.

²⁷ Art. 73 VAT Code:

Shall be punished with imprisonment of eight days to two years and with a fine of EUR 250 to EUR 500,000, or with one of those penalties, the person who with fraudulent intent or with the intent to harm, violates the provisions of this Code [i.e. the VAT Code] or of the decrees adopted for its implementation.’

If the offences mentioned in the first paragraph were committed in the context of serious tax fraud, organised or otherwise, the offender shall be punished with imprisonment of eight days to five years and a fine of EUR 250 to EUR 500,000, or with one of those penalties.

Tax fraud is in any event considered serious when the offences referred to in the first paragraph, are linked to the territory of at least two Member States and cause damage of at least 10,000,000 euros.

²⁸ Art. 73 nonies VAT Code:

The attempt to commit an offence referred to in Article 73, paragraph 3 shall be punished with imprisonment of eight days to three years and a fine of EUR 26 to EUR 50,000, or with one of those penalties.

Similarly, with regard to the **liability of legal persons**, Belgium is compliant with Article 6 of the PIF Directive, having already adopted compliant provisions prior to the Directive's enactment (Art. 5 of the Belgian Criminal Code²⁹).

The national expert underlined that: *“under Belgian criminal law, corporate criminal liability is autonomous or direct in nature, whereas the liability regime under EU law is indirect (Art. 6(1) PIF Directive) and functional (Art. 6(2) PIF Directive) in nature. While EU law does not require that the mens rea element is established on the part of the legal person, this is a requirement under Belgian criminal law. In this sense, the scope of Belgian criminal law is stricter, but it also does more justice to the efforts made by a legal person to prevent offences and to comply with the law. Moreover, contrary to EU law which confines cases of liability to the offenses committed by legal representatives of the legal person or other natural persons in a leading position, Belgian criminal law does not require this. An offense can be committed by any natural person, even a lower-level employee, and there is no requirement to identify the natural person nor to establish the offense on his part”.*

In particular, Belgium provides for the following sanctions (as indicated by **Art. 9 of the PIF**):

- criminal fine: EUR 500 EUR – EUR 1,000,000

For legal persons, the fine is identical for normal and serious VAT fraud, due to the conversion mechanism of Article 41 bis, paragraph 1 of the Criminal Code. This mechanism is to be applied to calculate the criminal fines applicable to legal persons.

Furthermore, it is important to note that these legal fines do not correspond to the actual amounts to be paid by convicted offenders. When sentenced to a fine, the amount of the fine needs to be multiplied by eight. This figure corresponds to the currently applicable ‘opdécimes’ (namely 70, which means that per euro, 7 euros need to be added) that apply to all criminal fines, save exceptions. This mechanism of additional “opdécimes”, which was first introduced in 1921 following the French example, allows the legislator to easily adjust the amount of all criminal fines to the changing costs of living and currency depreciation (inflation), this ensures that fines maintain their deterrent effect [see Article 1 of the Act of 5 March 1952].

The **other sanctions** foreseen are:

- placing under judicial supervision. This is only possible if:
 1. the criminal court decides to suspend the formal conviction and if it makes this decision conditional on several probational measures (Art. 3 and 18 bis of the Act of 29 June 1964);
 2. the legal person is convicted to a suspended sentence and if the criminal court imposes probational measures (Art. 8 and 18 bis of the Act of 29 June 1964).
- temporary or permanent closure of establishments that have been used for committing the criminal offense. Article 73ter, § 1, paragraph 2 VAT Code provides the criminal court with

²⁹ Art. 5 of the Criminal Code:

‘Any legal person is criminally liable for those offences which are either intrinsically linked to the achievement of its purpose or the defense of its interests or which, as evidenced by the concrete circumstances, have been committed on its behalf.

The following shall be assimilated with legal persons:

1° partnerships.

2° legal persons in formation.

The criminal liability of legal persons does not exclude that of natural persons, who are perpetrators of the same acts or participated in them.

the possibility to close an establishment for three months to five years in case of conviction of the person who is the director, a member or employee of the legal person. In most cases, this person is thus a natural person (except when the director would be another legal person). Therefore, the closure of establishments is not considered a criminal penalty for the company/legal person whose establishment(s) that is (are) closed, but rather a criminal penalty for the natural person who is the director, member, or an employee of the company. In the event the convicted person is a legal person (which is theoretically possible, but less frequent – see above), the closure of the establishment can be considered a criminal penalty for the legal person.

- publication of the judgment (Art. 73 septies VAT Code);
- professional ban or disqualification order. Art. 1, (i) of the Royal Decree No. 22 of 24 October 1934, which essentially excludes the legal person from being the director of another Belgian legal person or Belgian establishment of a foreign legal person. Art. 73ter, § 1 VAT Code: In case the offense is committed by a tax advisor, accountant or related profession, the criminal court can prohibit to exercise this profession for three months up to five years.

Finally, Belgian national legislation contains an **aggravating circumstance** for VAT fraud committed in the context of **organised crime**, as provided for by Article 8 of the PIF Directive [see art.73 VAT Code].

Bulgaria

Bulgaria is compliant with Article 3 of the PIF Directive, which concerns the criminalization of the commission of fraud to the detriment of the EU's financial interests. Bulgaria has achieved compliance **amending its pre-existing legislation**.

About the **objective element** of the crime, Bulgarian national legislation prescribes specific conducts, and binding actions in their criminal codes (articles from 253 to 260c, Bulgarian Criminal Code). Bulgaria prescribes all the conducts indicated in Article 3 of the PIF Directive, and adds others: refer to the hypothesis contained in Articles 245b³⁰ (misuse of European Union funds) and 258³¹ (obstruction of revenue authorities) of the Criminal Code and in Art. 83a³² and foll. (to 83g)

³⁰ Article 254b Criminal Code:

(New, SG No. 24/2005)

(1) (Amended, SG No. 26/2010) A person who uses any financial resources received from funds belonging to the European Union or such provided by the European Union to the Bulgarian State for any purpose other than as intended, shall be punished by imprisonment from one to six years.

(2) (Amended, SG No. 26/2010) If an official orders commission of the act referred to in the preceding paragraph, the punishment shall be imprisonment from two to eight years, and the court may deprive the convict of rights under Items 6 and 7 of Article 37 (1).

³¹ Article 258 Criminal Code:

(Amended, SG No. 28/1982, repealed, SG No. 10/1993, new, SG No. 62/1997)

(1) (Amended, SG No. 33/2011, effective 27.05.2011) A person who unlawfully creates obstructions to the revenue authorities in implementation of their lawful duties, shall be punished by imprisonment for up to three years and a fine from BGN 1,000 to 2,000.

(2) Should the deed under paragraph (1) be committed by force or threat, the punishment shall be imprisonment from one to six years and a fine from BGN 2,000 to 5,000.

³² Article 83a Administrative Violations and Sanctions Act

from the Administrative Violations and Sanctions Act (liability of legal entities for administrative violations).

With regard to the subjective element, Bulgaria provides that **only intentional acts** are punishable.

Bulgaria is compliant with the **required sanctions** for the commission of fraud, described in Art. 7 of the Directive, in particular compliance with the required maximum penalty of at least 4 years imprisonment in cases where the fraud committed against the financial interests of the EU has led to a loss of more than 100.000 € (threshold established for the “considerable damage”). Bulgaria meets the requirements and provides for a **maximum sentence of 6 years imprisonment**.

Lastly, as already explained, Annex 3 was dedicated to the assessment of compliance with Art. 6 of the PIF Directive, involving the **liability of legal persons**: 23 States out of 25, whether through amendments, new disciplines, or because they were already compliant, correctly transposed the

(New, SG No. 79/2005) [...]

A legal person, which has enriched itself or would enrich itself from a crime under Articles 108a, 109, 110 (preparations for terrorism), Articles 142 - 143a, 152(3) item 4, Articles 153, 154a, 155, 155a, 156, 158a, 159 - 159d, 162 (1) and (2), 164 (1), 171 (3), 172a - 174, 201 - 203, 209 - 212a, 213a, 214, 215, 216 (3), 225c, 227 (1) - (5), 242, 243, 244, 244a, 246(3), 248a, 250, 252, 253, 254b, 255, 255a, 255b, 256, 260a - 260c, 278c - 278e, 280, 281, 282 283, 301 - 307, 307b, 307c, 307d, 308 (3), 319a - 319f, 320 - 321a, 327, 352, 352a, 353b - 353f, 354a - 354c, 356j and 419a of the Criminal Code, as well as from all crimes, committed under orders of or for implementation of a decision of an organized criminal group, when they have been committed by:

1. an individual, authorized to formulate the will of the legal person.
 2. an individual, representing the legal person.
 3. an individual, elected to a control or supervisory body of the legal person,
- or

4. (amended, SG No. 81/20.10.2015, effective 21.11.2015) an employee to whom the legal person has assigned a certain task, when the crime was committed during or in connection with the performance of such task, shall be punishable by a financial penalty of up to BGN 1,000,000, but not less than the equivalent of the benefit, where the latter is of a financial nature; a penalty of up to BGN 1,000,000 shall also be imposed where the benefit is not of a financial nature or its amount cannot be established.

(2) (New, SG No. 81/2015, effective 21.11.2015) Such financial penalty shall also be imposed to legal persons not established in the territory of the Republic of Bulgaria where the crime referred to in paragraph 1 has been committed in the territory of the Republic of Bulgaria.

(3) (Renumbered from Paragraph 2, SG No. 81/2015, effective 21.11.2015) The financial penalty shall also be imposed on the legal person in the cases, when the persons under paragraph 1, items 1, 2 and 3 have abetted or assisted the commission of the above acts, as well as when the said acts were stopped at the stage of attempt.

(4) (Renumbered from Paragraph 3, amended, SG No. 81/2015, effective 21.11.2015) The financial penalty shall be imposed regardless of the materialization of the criminal responsibility of the accessories to the criminal act under paragraph 1.

(5) (New, SG No. 109/2020, effective 23.12.2021) When determining the amount of the financial penalty, the gravity of the crime, the financial state of the legal entity, the assistance rendered for disclosing the crime and for compensation of the damages of the crime, the amount of the benefit and other circumstances shall be taken into consideration.

(6) (Renumbered from Paragraph 4, amended, SG No. 81/2015, effective 21.11.2015, renumbered from Paragraph 5, SG No. 109/2020, effective 23.12.2021) The direct or indirect benefit derived by the legal person from the crime under paragraph 1 shall be confiscated in favor of the state, if not subject to return or restitution, or forfeiture under the procedure of the Criminal Code. Where the effects or property that were the object of the crime are missing or have been expropriated, their BGN equivalent shall be adjudged.

(7) (Renumbered from Paragraph 5, SG No. 81/2015, effective 21.11.2015, renumbered from Paragraph 6, SG No. 109/2020, effective 23.12.2021) Financial penalties under paragraph 1 shall not be imposed on states, state bodies and local self-government bodies, as well as on international organizations.

(8) (New, SG No. 109/2020, effective 23.12.2021) The liability of a legal entity shall be extinguished upon the expiration of a time limit equal to the time limit under Article 81 (3) of the Penal Code, considered as of the date of commission of the crime, from which the legal entity benefited or would have benefited.

PIF Directive regarding these aspects. Bulgaria is one of those: the country amended its previous legislation to reach the compliance.

In addition to the **custodial sentence**, **Bulgaria provides for administrative fines** (see also Art. 83a, Administrative Violations and Sanctions Act). They are up to BGN 1,000,000, but not less than the equivalent of the benefit illegally obtained.

Finally, Bulgaria's national legislation contains an **aggravating circumstance** for VAT fraud committed in the context of **organised crime**, as provided for by Article 8 of the PIF Directive. The punishment for this crime, also committed by organized criminals, is also foreseen in Article 83a of the Administrative Violations and Sanctions Act.

Croatia

Croatia did not directly transpose the Directive: **had implemented some amendments to its previous legislation, but still not meet the requirements**. In 2021, European Commission initiated an infringement procedure against Croatia for this reason.

With regard to the objective element of the crime, Croatia national legislation prescribe **specific conducts**, and binding actions in their criminal codes. These conducts are all the conducts indicated in Article 3 of the PIF Directive (i.e. the use or presentation of false, incorrect, or incomplete statements or documents, the misapplication of funds, assets, or benefits) except for:

Non-disclosure of VAT-related information in violation of a specific obligation;

The presentation of correct VAT-related statements for the purposes of fraudulently disguising the non-payment or wrongful creation of rights to VAT refunds.

The criminal offenses referred to in Art. 3 of the PIF Directive, which protects the financial interests of the European Union, corresponding to national criminal offences: evasion of taxes or customs

duties (art. 256 of the Criminal Code³³), subsidy fraud (Art. 258 of the Criminal Code³⁴), and fraud in business operations (Art. 247 of the Criminal Code³⁵).

With regard to the subjective element, Croatia provides that **only intentional acts** are punishable.

Croatia is compliant with the required sanctions for the commission of fraud, described in Art. 7 of the Directive, in particular compliance with the required maximum penalty of at least 4 years imprisonment in cases where the fraud committed against the financial interests of the EU has led to a loss of more than 100.000 € (threshold established for the “considerable damage”). Croatia meets the requirements and provides for a **maximum sentence of 5 years imprisonment, up to 10 in case of fraud with significant damage, when acting on behalf of a legal entity.**

Lastly, respect the compliance with Art. 6 of the PIF Directive, Croatia already foreseen this kind of responsibility, even before the PIF Directive.

Finally, Croatian national legislation contains an **aggravating circumstance** for VAT fraud committed in the context of **organised crime**, as provided for by Article 8 of the PIF Directive.

³³ Article 256 C.C.:

Tax or customs evasion

(1) Whoever, with the aim of having him or another person completely or partially avoid paying taxes or customs duties, provides incorrect or incomplete information about income, items or other facts that influence the determination of the amount of tax or customs liability, or whoever with the same aim in the case of mandatory report does not report the income, object or other facts that influence the determination of the tax or customs liability, and as a result the tax or customs liability is reduced or not determined in an amount that exceeds 2,654.46 euros, shall be punished by imprisonment from six months to five years.

(2) The penalty from paragraph 1 of this article shall be imposed on anyone who uses a tax relief or customs privilege in the amount of more than 2,654.46 euros contrary to the conditions under which he received it.

(3) If the criminal offense referred to in paragraphs 1 and 2 of this Article led to the reduction or non-determination of tax or customs liability on a large scale, the perpetrator will be punished with imprisonment from one to ten years.

(4) The provisions from paragraphs 1 to 3 of this article shall also be applied to the perpetrator who, in the actions described in them, reduces the funds of the European Union.

³⁴ Article 258 C.C.:

Subsidy fraud

(1) Whoever, with the aim of obtaining state aid for himself or for another, provides the state aid provider with incorrect or incomplete information on the facts on which the adoption of a state aid decision depends or fails to inform the state aid provider of changes important for the adoption of a decision on state aid, shall be punished by imprisonment for a term of six months to five years.

(2) The penalty referred to in Paragraph 1 of this Article shall be imposed on anyone who uses funds from the approved state aid contrary to their purpose.

(3) If, in the case referred to in Paragraph 1 of this Article, the offender acted with the aim of obtaining large-scale state aid or, in the case referred to in Paragraph 2 of this Article, used large-scale state aid, shall be punished by imprisonment for a term of one to ten years.

(4) Whoever, in the cases referred to in Paragraph 1 of this Article, voluntarily prevents the adoption of a decision on state aid, may be released from punishment.

(5) Subsidies and aids approved from the European Union funds shall be treated as state aid within the meaning of this Article.

³⁵ Article 247 C.C.:

(1) Whoever, in business operations, with the aim of obtaining unlawful property gain for the legal person he represents or another legal person, misleads someone by false presentation or concealment of facts or keeps him in error, thereby leading him to do or not to do something to the detriment of his own or someone else's property, shall be punished by imprisonment for a term of six months to five years.

(2) If the criminal offence referred to in Paragraph 1 of this Article has caused significant damage, the offender shall be punished by imprisonment for a term of one to ten years.

Cyprus

Cyprus is compliant with Article 3 of the PIF Directive, which concerns the criminalization of the commission of fraud to the detriment of the EU's financial interests. In February 2022, the European Commission started an infringement procedure against Cyprus. Cyprus, to achieve compliance, introduced an **entirely new legislation**.

Cyprus' national legislation classifies VAT fraud as a general offence (**free form**), which means that no specific conduct or actions are explicitly defined. The crime is foreseen by Article 4, L. 4762/2020 as amended by I. 114/2021

About the subjective element, Cyprus applies liability for **both intent and negligence**.

Annex 2 delved into compliance with the required sanctions for the commission of fraud, described in art. 7 of the Directive. Specifically, the question concerned compliance with the required maximum sentence of at least 4 years of imprisonment in cases where the fraud committed against the financial interests of the EU had led to damage of over 100.000 € (threshold established for the "considerable damage". Cyprus meets the requirements and provides for a **maximum sentence of 7 years imprisonment**.

Lastly, Annex 3 was dedicated to the assessment of compliance with Art. 6 of the PIF Directive, involving **the liability of legal persons**: Cyprus is compliant and enacted new legislations to achieve compliance.

More specifically, the **sanctions** foreseen in Cyprus for VAT fraud committed by legal persons are:

- criminal fine (€50.000);
- detention;
- temporary or permanent disqualification from the practice of commercial activities;
- placing under judicial supervision;
- judicial winding-up;
- temporary or permanent closure of establishments that have been used for committing the criminal offense.

Finally, Cyprus's national legislation contains an **aggravating circumstance** for VAT fraud committed in the context of **organised crime**, as provided for by Article 8 of the PIF Directive.

Czech Republic

The Czech Republic (CR) has **achieved compliance with Article 3 of the PIF Directive**, which mandates the criminalization of fraud against the financial interests of the European Union. **Compliance was reached through the amendment of pre-existing legal frameworks**, ensuring alignment with the Directive's requirements. The key provision is Art. 260 Criminal Code³⁶ (Damage

³⁶ § 260 Criminal Code

Damage to the financial interests of the European Union

(1) Whoever makes, uses or presents false, incorrect or incomplete documents, gives false, incorrect or incomplete information or conceals documents or information, thereby permits the unauthorised use or retention of funds deriving from the budget of the European Union or budgets managed by or on behalf of the European Union, or the diminution of the resources of any such budget, or permits the unauthorised use

to the financial interests of the EU). The Czech Criminal Code was amended by Act No. 315/2019 Sb. that implemented the additional requirements of PIF. The second important provision is included in Art. 240 Criminal Code³⁷ (Tax, fee, and similar mandatory payment evasion).

Referring to classification and the objective element of the crime, in Czech national legislation, VAT fraud is broadly classified as a **general offense** ("free-form"). This classification does not explicitly delineate specific behaviors or actions but rather encompasses a wide range of fraudulent activities under the general framework of tax evasion (Art. 260 of the Criminal Code, as amended by Art. 260 of the Penal Code, as amended by Act No. 315). So, there is no autonomous offense of VAT fraud, but this conduct falls within the broader category of tax evasion.

Regarding the **subjective elements** required for criminal liability, Czech law stipulates that only **intentional acts** are punishable, excluding negligence or unintentional breaches.

With respect to compliance with the required sanctions for the commission of fraud, described in art. 7 of the Directive; Czech Republic meets the requirements and provides for a **maximum sentence of 5 years imprisonment**. To be more complete, the sanctions are up to 5 years in case of criminal offense under § 260 and up to 8 years under criminal offense under § 240. Moreover, there are differences based on the amount of damage caused, as also provided for other offenses [see Article 138 of the Criminal Code³⁸].

or retention of property acquired from the budget of the European Union or budgets managed by or on behalf of the European Union, shall be liable to a term of imprisonment of up to three years, to a prohibition of activities or to confiscation of property.

(2) Anyone who misuses funds deriving from the budget of the European Union or budgets managed by or on behalf of the European Union, property acquired from the budget of the European Union or budgets managed by or on behalf of the European Union, or diminishes the resources of any such budget, shall be punished in the same way.

(3) Imprisonment for one to five years or a fine shall be imposed if the offender causes greater damage by an act referred to in paragraph 1 or paragraph 2.

(4) Imprisonment for two years to eight years will be imposed on the offender,

a) commits the act referred to in paragraph 1 or paragraph 2 as a member of an organised group,
b) commits such an act as a person under a special obligation to defend the interests of the European Union, or
c) if he causes substantial damage by such an act.

(5) imprisonment for five to ten years shall be imposed if, by an act referred to in paragraph 1 or 2, the offender causes damage on a large scale.

³⁷ § 240 Criminal Code

Tax, fee, and similar mandatory payment evasion

(1) Whoever, on a large scale, evades a tax, duty, social security contribution, state employment insurance contribution, accident insurance contribution, health insurance contribution, fee or other similar compulsory payment or extorts a benefit on any of these compulsory payments shall be punished by imprisonment for six months to three years or by prohibition of activity.

(2) The offender shall be punished by imprisonment for two years to eight years,

a) commits the act referred to in paragraph 1 with at least two persons,
b) if, in order to facilitate such an act, he violates an official closure, or
c) commits such an act on a substantial scale.

(3) imprisonment for five to ten years shall be imposed on the offender,

a) if he commits the act referred to in paragraph 1 on a large scale, or
b) commits an act referred to in paragraph 2(c) in association with an organised group operating in more than one State.

(4) Preparation is punishable.

³⁸ § 138 Criminal Code

Limits on the amount of damage, benefit, cost to remedy environmental damage and value of the thing

(1) For the purposes of this Act means

a) not insubstantial damage amounting to not less than 10,000 CZK,
b) by a not minor damage amounting to at least 50,000 CZK,

The Czech Republic was already compliant with Article 6 of the PIF Directive, before its implementation [Section 7, Law n. 418/2011 about the **liability of legal persons**].

Czech law provides a comprehensive range of sanctions for VAT fraud, as required by **Article 9 of the PIF Directive**.

These sanctions encompass both criminal and non-criminal measures, demonstrating a robust approach to deterring and addressing such offenses:

- criminal fine (from 20 000 CZK to 1 460 000 000 CZK);
- non-criminal fine (confiscation of property);
- exclusion from entitlement to public benefits or aid;
- temporary or permanent exclusion from public tender procedures;
- temporary or permanent disqualification from the practice of commercial activities;
- judicial winding-up.

Finally, CR national legislation contains an **aggravating circumstance** for VAT fraud committed in the context of **organised crime**, as provided for by Article 8 of the PIF Directive.

Denmark

Concerning **compliance with Article 3 of the PIF Directive** did not transpose the Directive: among them, Denmark was not legally required to transpose it.

In Danish legislation VAT fraud is classified as a **general offense (free-form)**, meaning no specific behaviors or actions are explicitly defined.

In Denmark, tax fraud is defined as any intentional act or omission that results in the evasion or avoidance of taxes owed to the state. This includes:

- underreporting income or overstating deductions;
- concealing assets or sources of income;
- falsifying financial records or documents;
- failing to file tax returns or providing inaccurate information

Danish law distinguishes between tax evasion and tax avoidance. Tax evasion involves illegal actions to reduce tax liability, while tax avoidance refers to legal methods of minimizing taxes. The legal framework governing tax fraud in Denmark is primarily contained in the Danish Tax Control Act (Lov om Skattekontrol) and in the Danish Criminal Code (Straffeloven).

With regard to the subjective element, Denmark applies liability for **both intent and negligence**.

c) greater damage amounting to at least 100,000 CZK,

d) substantial damage amounting to at least 1,000,000 CZK, and

e) damage of great magnitude amounting to at least 10,000,000 CZK.

(2) The amounts set forth in paragraph 1 shall be used mutatis mutandis to determine the amount of the benefit, the cost to remedy the environmental damage, and the value of the property.

About the compliance with the required sanctions for the commission of fraud, described in art. 7 of the Directive (sanctions for natural persons), Denmark meets the requirements and provides for a **maximum sentence of 4 years imprisonment**.

Regarding compliance with Art. 6 of the PIF Directive, involving the **liability of legal persons** Denmark did not transpose because it is not legally required to, being however bound by the PIF Convention.

As regards the **sanctions set out in Article 9 of the PIF Directive**, these are mainly criminal, although there are also non-criminal (administrative or civil) ones. In Danish legislation, the following penalties are provided for about legal persons found liable under Article 6:

- criminal fine (not specified);
- non-criminal fine (not specified);
- judicial winding-up;
- temporary or permanent closure of establishments that have been used to commit the offense.

There is a **general aggravating circumstance** in the Danish Criminal Code, under Article 81³⁹, which provides for an increased penalty in cases where the offense is committed in an organized manner.

Estonia

Even though Estonia did not respond to the questionnaire prepared for the EU Cyber VAT fraud project, it has nonetheless been possible to assess its **compliance** with the PIF Directive and **Article 3**. Specifically, the European Commission initiated an infringement procedure against Estonia in May 2022 for its non-compliance with the Directive.

Estonia has adapted its Criminal Code to include specific financial crimes, including tax fraud and VAT fraud, by the provisions of the PIF Directive, specifically in Article 389(1)⁴⁰.

³⁹ § 81 C.C.:

It should at fixing the penalty generally included as an aggravating circumstance, 1) the offender previously convicted of importance to the case, 2) that the act is done by several jointly, 3) that the offense is particularly planned or part of comprehensive crime, 4) that the perpetrator intended that the act would have considerable more serious consequences than the turns, 5) the offender has shown particular ruthlessness, 6) that the ministry is rooted in people's ethnic origin, religion, sexual orientation or the like, 7) that the act is a consequence of the victim's legal utterances in public debate, 8) the offense is committed in the conduct of public officials or abuse of position or special relationship of trust, moreover, 9) the offender has got someone else to help the ministry by force, fraud or exploitation of his young age or significant financial or personal difficulties, lack of knowledge, carelessness or an existing relationship, 10) that the perpetrator has used victim's defenseless position, 11) the offense is committed by a person undergo, imprisonment or other punishment of a custodial nature, 12) the offense is committed by a former inmate of the institution or person employed by the institution.

⁴⁰ § 389(1) C.C.:

Concealment of tax liability and unfounded increase of claim for refund
[RT I, 12.07.2014, 1 - entry into force 01.01.2015]

(1) Failure to submit information or submission of incorrect information to tax authorities for the purpose of reduction of an obligation to pay a tax or obligation to withhold, or increase a claim for refund, if a tax liability or obligation to withhold is thereby concealed or a claim for return is unfoundedly increased by an amount corresponding to or exceeding major damage, is punishable by a pecuniary punishment or up to five years' imprisonment.

In this article, there are foreseen the **conducts** required for the commission of fraud, **very broad** ("Failure to submit information or submission of incorrect information to tax authorities for reduction of an obligation to pay a tax or obligation to withhold, or increase a claim for refund, if a tax liability or obligation to withhold is thereby concealed or a claim for return is unfoundedly increased by an amount corresponding to or exceeding major damage").

The **subjective element requires the intention**.

The punishment is higher than the provision of the Directive: an economic sanction or **up to 5 years imprisonment**, which become **up to 10 years for the most serious offenses**. The imprisonment is **up to 7 years**, if a tax liability or obligation to withhold is thereby concealed or a claim for refund is unfoundedly increased by an amount corresponding to particularly great damage.

Regarding Art. 6 of the PIF Directive, involving the **liability of legal persons**, Estonia is compliant [v. art. 389 (1) para. 3]. Other sanctions may also be applied, such as the extended confiscation of assets or property acquired through the crime or the deletion of a legal person from the register.

Finland

In terms of compliance with Article 3 of the PIF Directive, **Finland is compliant**, as stated in Government Proposal No. 231/2018, but it is unclear how compliance was achieved; according to the Finnish national expert, no substantial changes were required to achieve compliance, suggesting that the existing framework and legislation are already in line with the requirements of the Directive.

However, it should be noted that initially, in December 2021, the European Commission started an infringement procedure against Finland regarding the transposition of the PIF directive. The procedure was closed only after the explanatory replies from the Finnish government.

As regards compliance with the sanctions required by **Article 7 of the PIF Directive** for natural persons committing VAT fraud, in the case of Finland, although the maximum penalty is two years imprisonment and could therefore be incompatible, **compliance with Article 7 of the PIF Directive seems to be achieved by the joint provision of other articles of the Finnish Penal Code (RL)**, in particular, fiscal offenses and offenses against the public administration: aid fraud (RL 29:5), abuse of aid (RL 29:7), fraud (RL 36:1), tax evasion (RL 29:1), money laundering (RL 32:6), giving a bribe (RL 16:13), giving a bribe to a member of parliament (RL 16:14a), taking a bribe (RL 40:1), accepting a bribe as a member of parliament (RL 40:4) and abuse of office (RL 40:7).

With regard to the subjective element, Finland applies liability for **both intent and negligence**.

(2) The same act, if a tax liability or obligation to withhold is thereby concealed or a claim for refund is unfoundedly increased by an amount corresponding to particularly great damage, is punishable by one to seven years' imprisonment.

(3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

(4) For criminal offence provided for in subsection (2) of this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of § 832 of this Code.

About compliance with Art. 6 of the PIF Directive, involving the liability of legal persons, **Finland is compliant and reached compliance by amending its previous legislation**, specifically Section 9 of the Finnish Criminal Code⁴¹, as amended by Article 10 L. 2019/368.

As regards the **sanctions** provided for in **Article 9 of the PIF Directive** about legal persons recognised as responsible under Article 6, Finnish legislation provides for a criminal fine of 850-850,000 euros.

Concerning the **aggravating circumstance**, Finland reports on the parliamentary discussion, which considered that the provision of an aggravating circumstance in the case of VAT fraud committed by a criminal organisation was not necessary, as they already comply with the Framework Decision 2008/841/JHA. Thus, Finland does not apply directly the aggravating circumstance provided for in Art. 8 of the PIF Directive, because it is already covered by Framework Decision 2008/841/JHA. This provision allows for increased penalties and the application of more severe sanctions when crimes are committed by organized criminal groups, as well as in the case of VAT fraud committed by organised groups.

France

According to the answers of the French national expert, France has **not transposed the directive** into its national legal framework, at least in regard to **Article 3 of the PIF Directive**. The existing legislation is inadequate, and no amendments have been made to address the requirements of the directive.

However, it should be noted that no infringement procedure has ever been initiated by the European Commission against France for this reason, likely considering the pre-existing legislation to be sufficient.

For the national expert, although criminal legislation can be applied to certain VAT fraud crimes, such legislation does not specifically address this crime and is applied generally for fraud (Art. 313-

⁴¹ Section 9 C.C.:

Corporate criminal liability

If, under this chapter, Finnish law applies to the offence, Finnish law applies also to the determination of corporate criminal liability.

1⁴², 313-2⁴³, 313-3⁴⁴, 441-6⁴⁵ criminal code) and for money laundering (Art. 324-1 C.C⁴⁶). As a result, not all specific conduct related to VAT fraud can be directly covered by the criminal code, as they are provided for in tax and administrative legislation.

Among the crimes related to VAT, there are:

- forgery of tax documents;
- false statements or intentional omissions and/or misuse of fictitious identities or companies;
- organized Fraud Schemes;
- tax evasion.

⁴² Article 313-1 C.C.:

Fraud - (Updated by Law No. 2019-222 of March 23, 2019)

A person who, by any means, engages in fraudulent practices to mislead someone with the aim of obtaining an undue financial advantage, either for themselves or for another person, shall be punished by imprisonment for up to 5 years and a fine of up to 375,000 euros.

This penalty can be increased to a prison sentence of up to 7 years and a fine of up to 750,000 euros when the offense is committed as part of a criminal organization or when the damage caused is particularly significant.

If the fraud targets a public institution, the penalties can be even more severe.

⁴³ Article 313-2 C.C.:

Fraudulent Misrepresentation and False Documents

Any person who, with the intention of obtaining an unlawful benefit for themselves or for others, has:

(1) Forged or altered a document with the aim of committing fraud.

(2) Presented or used a forged or altered document to deceive someone in order to obtain money or an asset.

(3) Used a document known to be false to gain or attempt to gain undue advantage, shall be punished by imprisonment for up to 5 years and a fine of up to 375,000 euros.

If the offense is committed by an organized criminal group, the penalties may be more severe, including longer imprisonment or higher fines.

⁴⁴ Article 313-3 C.C.:

Aggravating Circumstances for Fraud

The penalties set forth in Article 313-1 are increased in the following cases:

When the fraud involves the use of false documents or the creation of false information.

When the fraud is committed by an organized criminal group or when the offender has committed multiple offenses related to fraud.

When the fraud causes damage to a public institution or significant financial losses.

In such cases, the punishment can be extended to imprisonment for up to 10 years and a fine of up to 1,000,000 euros.

⁴⁵ Article 441-6 C.C.:

The act of obtaining a document from a public administration or from an organization entrusted with a public service mission, by any fraudulent means, that is intended to establish a right, identity, or status, or to grant an authorization, is punishable by two years of imprisonment and a fine of 30,000 euros.

The same penalties apply to the act of knowingly providing a false or incomplete declaration with the intention of obtaining, or attempting to obtain, for oneself or for another person, from a public authority, a social protection organization, or an organization entrusted with a public service mission, an allowance, benefit, payment, or undue advantage.

⁴⁶ Article 324-1 C.C.:

Money laundering is the act of facilitating, by any means, the false justification of the origin of goods or income of the author of a crime or offense that has provided him with a direct or indirect profit.

Money laundering also includes providing assistance to an operation involving the placement, concealment, or conversion of the direct or indirect proceeds of a crime or offense.

Money laundering is punishable by five years of imprisonment and a fine of 375,000 euros.

Finally, article 113-14 of the French Criminal Code⁴⁷ deals with the application of French criminal law to this offense committed abroad if it affects the financial interests of the European Union.

In the French legal system, there is no specific VAT fraud offense, but there are various broader crimes that can also be applied to combat VAT fraud, and all the conducts outlined in **Article 3 of the Directive are effectively encompassed**.

Regarding the **subjective elements** required for criminal liability, French law stipulates that only **intentional acts** are punishable, excluding negligence or unintentional breaches.

As regards compliance with the sanctions required by Article 7 of the PIF Directive for natural persons committing VAT fraud, it is noted that the punishments **vary according to the severity of the offense**. They can include prison sentences ranging from a few months to several years, depending on the amount of tax evaded, the existence of aggravating circumstances (such as the use of forged documents or the formation of a criminal organization to commit tax fraud), and the recurrence of the crime. For this reason, the French expert considered that the national legislation was **not compliant with Article 7** of the PIF Directive because it is not always possible to establish whether the penalty for VAT fraud exceeds the threshold set by the Directive itself.

According to the national expert, with respect to compliance with **Art. 6 of the PIF Directive**, involving the liability of legal persons, France is not compliant, since **has not yet amended its legislation**.

However, it should be highlighted that in France, there is the possibility of holding legal persons responsible for crimes, as provided for by Articles 121-1⁴⁸ and 121-2⁴⁹ of the Penal Code.

⁴⁷ Article 113-14 C.C.:

By way of derogation from the second paragraph of Article 113-6, French criminal law applies in all circumstances, and the second sentence of Article 113-8 does not apply, to the following offenses committed abroad by a French national or by a person who habitually resides or conducts all or part of their economic activity in French territory, when they harm the revenue, expenses, or assets that fall under the budget of the European Union, the budgets of the institutions, bodies, and agencies of the European Union, or the budgets directly managed and controlled by them:

1° Offenses of fraud as defined in Section 1 of Chapter III of Title I of Book III.

2° Offenses of breach of trust as defined in Section 1 of Chapter IV of Title I of Book III.

3° Offenses of misappropriation, embezzlement, or destruction of property as defined in Articles 432-15 and 433-4.

4° Offenses of corruption as defined in Articles 432-11 and 433-1, as well as, without prejudice to Article 435-11-2, Articles 435-1 and 435-3.

5° Offenses of smuggling, fraudulent importation or exportation as defined in Article 414-2 of the Customs Code.

6° Offenses of money laundering as defined in Section 1 of Chapter IV of Title II of Book III of the offenses mentioned in this article.

For the prosecution of a person who has committed, on French territory, as an accomplice, an offense referred to in 1° to 6° committed abroad and affecting the financial interests of the European Union mentioned in the first paragraph of this article, the conditions set forth in Article 113-5 do not apply.

⁴⁸ Article 121-1 C.C.:

A person who has committed a criminal offense is subject to criminal penalties.

The provisions of the Penal Code shall apply to offenses committed by individuals or legal entities, as specified in the law.

⁴⁹ Article 121-2 C.C.:

Legal entities, excluding the State, are criminally liable, in accordance with the distinctions set out in Articles 121-4 to 121-7, for offenses committed on their behalf by their organs or representatives.

However, local authorities and their groupings are only criminally responsible for offenses committed in the exercise of activities that are subject to public service delegation agreements.

Regarding the sanctions as indicated in Article 9 of the PIF Directive, France provides:

- criminal fine (article 131-38, 313-9, 313-1,313-2 and 313-3);
- temporary or permanent exclusion from public tender procedures;
- temporary or permanent disqualification from the practice of commercial activities;
- placing under judicial supervision;
- temporary or permanent closure of establishments that have been used for committing the criminal offense.

France does not specifically apply the aggravating circumstance outlined in Article 8 of the PIF Directive for VAT fraud. However, various provisions in the French Criminal Code include aggravating circumstances in cases where the crime is committed by an organized criminal group.

Germany

With respect to **compliance with Article 3 of the PIF Directive**, Germany is compliant by **amendment of a pre-existing discipline.**

The national expert highlighted that there are more provisions for the guarantee of the protection of the EU's financial interests, for instance, general provisions on fraud, computer fraud and

The criminal liability of legal entities does not exclude the liability of natural persons who are the perpetrators or accomplices of the same acts, subject to the provisions of the fourth paragraph of Article 121-3.

subsidy fraud. The amendments are related to Sections 263⁵⁰, 263a⁵¹, 264⁵², 266⁵³ German Criminal Code.

⁵⁰ Sec. 263 German Criminal Code:

Fraud

(1) Whoever, with the intention of obtaining an unlawful pecuniary benefit for themselves or a third party, damages the assets of another by causing or maintaining an error under false pretenses or distorting or suppressing true facts incurs a penalty of imprisonment for a term not exceeding five years or a fine.

(2) The attempt is punishable.

(3) In especially serious cases, the penalty is imprisonment for a term of between six months and 10 years. An especially serious case typically occurs where the offender:

1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of forgery of documents or fraud,
2. causes a major financial loss to or acts with the intention of placing many persons in danger of financial loss by the continued commission of fraud,
3. places another person in financial hardship,
4. abuses his or her powers or position as a public official or European official or
5. pretends that an insured event has happened after they or another person have set fire to an object of significant value or destroyed it, in whole or in part, by setting fire to it or caused the sinking or grounding of a ship.

(4) Section 243 (2) and sections 247 and 248a apply accordingly.

(5) Whoever commits fraud on a commercial basis as a member of a gang whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269 incurs a penalty of imprisonment for a term of between one year and 10 years, in less serious cases imprisonment for a term of between six months and five years.

(6) The court may make an order for the supervision of conduct (section 68 (1)).

⁵¹ Section 263a C.C.:

Computer fraud

(1) Whoever, with the intention of obtaining an unlawful pecuniary benefit for themselves or a third party, damages the property of another by influencing the result of a data processing operation by incorrectly configuring the computer program, using incorrect or incomplete data, making unauthorised use of data or taking other unauthorised influence on the processing operation incurs a penalty of imprisonment for a term not exceeding five years or a fine.

(2) Section 263 (2) to (6) applies accordingly.

(3) Whoever prepares an offence under subsection (1) by:

1. producing computer programs the purpose of which is to commit such an act or procures such programs for themselves or another, or
 2. producing, procuring for themselves or another, offering for sale, storing or supplying to other passwords or other security codes suited to committing such an act
- incurs a penalty of imprisonment for a term not exceeding three years or a fine.

(4) In the cases under subsection (3), section 149 (2) and (3) applies accordingly.

⁵² Section 264 C.C.:

Subsidy fraud

(1) Whoever:

1. furnishes an authority which is competent to approve a subsidy, or another agency or person involved in the subsidy procedure (subsidy giver), for themselves or another person, with incorrect or incomplete particulars regarding facts which are advantageous for themselves or the other person, such particulars being relevant for the granting of a subsidy,
 2. uses an object or cash benefit the use of which is restricted by legal provisions or by the subsidy giver in relation to a subsidy contrary to that restriction,
 3. withholds from the subsidy giver, contrary to the legal provisions relating to grants of subsidies, facts relevant to the subsidy or
 4. uses a certificate of entitlement to a subsidy or about facts relevant to a subsidy which was obtained by furnishing incorrect or incomplete particulars in a subsidy procedure
- incurs a penalty of imprisonment for a term not exceeding five years or a fine.

(2) In especially serious cases, the penalty is imprisonment for a term of between six months and 10 years. An especially serious case typically occurs where offenders

1. acquire, out of gross self-interest or by using forged or falsified documentation, an unjustified, large subsidy for themselves or another,

However, as subsidies in Germany are also granted as tax benefits and can therefore lead to a loss of revenue for the EU and fraud to the detriment of the financial interests is also committed via VAT, the criminal and administrative offense provisions of criminal tax law must also be taken into account. These can be found in the German Fiscal Code (Sections 370, 378, 379, 380, 382 Fiscal Code) and the German VAT Act (Sections 26a, 26c VAT Act). In particular, the VAT act contains, in article 26c⁵⁴, a regulation on penalizing the non-payment of VAT, which does not exist in Germany for other taxes.

Finally, in 2019, the German legislator passed a law to strengthen the protection of the European Union's financial interests (EU Financial Protection Strengthening Act – EUFinSchStG - Gesetz zur Stärkung des Schutzes der finanziellen Interessen der Europäischen Union) to close the last gaps in protection.

In Germany, VAT fraud is prosecuted for **both intent and negligence**.

2. abuse their powers or position as a public official or European official or
3. take advantage of the assistance of a public official or European official who abuses his or her powers or position.

(3) Section 263 (5) applies accordingly.

(4) In the cases under subsection (1) no. 2, the attempt is punishable.

(5) Whoever acts recklessly in the cases under subsection (1) nos. 1 to 3, incurs a penalty of imprisonment for a term not exceeding three years or a fine.

(6) Whoever voluntarily prevents the granting of a subsidy on the basis of the offence incurs no penalty under subsections (1) and (5). If the subsidy is not granted without any action on the offender's part, no penalty is incurred if the offender makes voluntary and earnest efforts to prevent the subsidy from being granted.

(7) In addition to a sentence of imprisonment of at least one year for an offence under subsections (1) to (3), the court may order the loss of the ability to hold public office and be elected in public elections (section 45 (2)). Objects relating to the offence may be confiscated; section 74a applies.

(8) 'Subsidy' within the meaning of this provision means:

1. a benefit from public funds under federal or Länder law for businesses or enterprises which, at least in part,

a) is granted without market-related consideration and

b) is intended to promote the economy,

2. a benefit from public funds under the law of the European Union, which is granted, at least in part, without market-related consideration.

A public enterprise is also deemed to be a business or enterprise within the meaning of sentence 1 no. 1.

(9) Facts are relevant to a subsidy within the meaning of subsection (1)

1. if they are designated as being relevant to a subsidy by law or by the subsidy giver on the basis of a law or

2. if the approval, granting, reclaiming, renewal or continuation of a subsidy or of an advantage of subsidisation is dependent on them for reasons of law or under the subsidy contract.

⁵³ Section 266 C.C.:

Embezzlement/Misuse

(1) Whoever abuses the power conferred on them by law, by commission of an authority or legal transaction to dispose of the assets of another or to make binding agreements for another, or whoever breaches their duty to safeguard the pecuniary interests of another which are incumbent upon them by reason of law, by commission of an authority, legal transaction or fiduciary relationship, and thereby adversely affects the person whose pecuniary interests they were responsible for, incurs a penalty of imprisonment for a term not exceeding five years or a fine.

(2) Section 243 (2), sections 247 and 248a, and section 263 (3) apply accordingly.

⁵⁴ Section 26c VAT Act:

Criminal provisions

A custodial sentence not exceeding five years or a monetary penalty shall be imposed on anyone who, in the cases referred to in section 26a (1), acts commercially or as a member of a gang that has joined together to commit such offences on an ongoing basis.

The **penalties** are dissuasive and provide for maximum prison sentences of at least five years for fraud, computer fraud, subsidy fraud, embezzlement and tax evasion, and up to 10 years for the cases covered by Art. 7 para. 3 of PIF Directive.

Regarding compliance with **Art. 6 of the PIF Directive**, involving the liability of legal persons, **Germany had already compliant provisions before the directive** (Articles 30⁵⁵ and 130⁵⁶ of Act on Regulatory Offense).

⁵⁵ Section 30 Act on Regulatory Offence:

Regulatory Fine Imposed on Legal Persons and on Associations of Persons

(1) Where someone acting:

1. as an entity authorised to represent a legal person or as a member of such an entity,
2. as chairman of the executive committee of an association without legal capacity or as a member of such committee,
3. as a partner authorised to represent a partnership with legal capacity, or
4. as the authorised representative with full power of attorney or in a managerial position as procura-holder or the authorised representative with a commercial power of attorney of a legal person or of an association of persons referred to in numbers 2 or 3,
5. as another person responsible on behalf of the management of the operation or enterprise forming part of a legal person, or of an association of persons referred to in numbers 2 or 3, also covering supervision of the conduct of business or other exercise of controlling powers in a managerial position, has committed a criminal offence or a regulatory offence as a result of which duties incumbent on the legal person or on the association of persons have been violated, or where the legal person or the association of persons has been enriched or was intended to be enriched, a regulatory fine may be imposed on such person or association.

(2) The regulatory fine shall amount:

1. in the case of a criminal offence committed with intent, to not more than ten million Euros,
2. in the case of a criminal offence committed negligently, to not more than five million Euros.

Where there has been commission of a regulatory offence, the maximum regulatory fine that can be imposed shall be determined by the maximum regulatory fine imposable for the regulatory offence concerned. If the Act refers to this provision, the maximum amount of the regulatory fine in accordance with the second sentence shall be multiplied by ten for the offences referred to in the Act. The second sentence shall also apply where there has been commission of an act simultaneously constituting a criminal offence and a regulatory offence, provided that the maximum regulatory fine imposable for the regulatory offence exceeds the maximum in accordance with the first sentence.

(2a) In the event of a universal succession or of a partial universal succession by means of splitting (section 123 subsection 1 of the Reorganisation Act [Umwandlungsgesetz]), the regulatory fine in accordance with subsections 1 and 2 may be imposed on the legal successor(s). In such cases, the regulatory fine may not exceed the value of the assets which have been assumed, as well as the amount of the regulatory fine which is suitable against the legal predecessor. The legal successor(s) shall take up the procedural position in the regulatory fine proceedings in which the legal predecessor was at the time when the legal succession became effective.

(3) Section 17 subsection 4 and section 18 shall apply mutatis mutandis.

(4) If criminal proceedings or regulatory fining proceedings are not commenced on account of the criminal offence or of the regulatory offence, or if such proceedings are discontinued, or if imposition of a criminal penalty is dispensed with, the regulatory fine may be assessed independently. Statutory provision may be made to the effect that a regulatory fine may be imposed in its own right in further cases as well. Independent assessment of a regulatory fine against the legal person or association of persons shall however be precluded where the criminal offence or the regulatory offence cannot be prosecuted for legal reasons; section 33 subsection 1 second sentence shall remain unaffected.

(5) Assessment of a regulatory fine incurred by the legal person or association of persons shall, in respect of one and the same offence, preclude a confiscation order, in accordance with sections 73 or 73c of the Penal Code or in accordance with section 29a, against such person or association of persons.

(6) On issuance of a regulatory fining notice, in order to secure the regulatory fine, section 111e subsection 2 of the Code of Criminal Procedure shall be applied on proviso that the judgment is substituted by the regulatory fining notice.

⁵⁶ Section 130 Act on Regulatory Offence:

Violation of obligatory supervision in operations and enterprises

The sanctions, indicated in **Article 9** of the PIF Directive and applicable in Germany are:

- non-criminal fine: 10 million euros for each offense;
- confiscation measures that may be imposed in addition to the fine;
- exclusion from entitlement to public benefits or aid;
- temporary or permanent exclusion from public tender procedures;
- temporary or permanent disqualification from the practice of commercial activities.

In Germany, there is also an **aggravating circumstance** for the commission of these crimes by organized criminal groups.

Greece

With respect to **compliance with Article 3 of the PIF Directive on the** commission of fraud to the detriment of the EU's financial interests, Greece has achieved compliance by the **introduction of new legislation**. Indeed, in December 2021, the European Commission initiated an infringement procedure.

The national expert highlighted that the Greek law establishes a “complex model” to protect EU financial interests, which includes:

- provisions aligning EU property protection with Greek public property laws, covering most offenses against EU financial interests under the Penal Code or the National Customs Code;
- subsidiary provisions for offenses not covered by existing criminal laws, applicable if heavier penalties are not already established;
- specific provisions to address cross-border VAT fraud, requiring new regulations for this type of crime.

Rather than creating a special criminal law like Law 2803/2000, Greece opted to address cross-border VAT fraud through Article 23⁵⁷ (passed by Law 4689/2000), providing a more focused and

(1) Whoever, as the owner of an operation or undertaking, intentionally or negligently omits to take the supervisory measures required to prevent contraventions, within the operation or undertaking, of duties incumbent on the owner and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as would have been prevented, or made much more difficult, if there had been proper supervision. The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel.

(2) An operation or undertaking within the meaning of subsection 1 shall include a public enterprise.

(3) Where the breach of duty carries a criminal penalty, the regulatory offence may carry a regulatory fine not exceeding one million Euros. Section 30 subsection 2 third sentence shall be applicable. Where the breach of duty carries a regulatory fine, the maximum regulatory fine for breach of the duty of supervision shall be determined by the maximum regulatory fine imposable for the breach of duty. The third sentence shall also apply in the case of a breach of duty carrying simultaneously a criminal penalty and a regulatory fine, provided that the maximum regulatory fine imposable for the breach of duty exceeds the maximum in accordance with the first sentence.

⁵⁷ Article 23 of Law 4689/2000:

“Whoever, during the execution of an organized plan involving transactions carried out in the territory of at least two (2) Member States of the European Union, results in a loss of VAT resources exceeding a total of ten million (10,000,000) euros a) by using or presenting false, incorrect/inaccurate or incomplete VAT

severe penalty. This choice aims to extend VAT protection to other EU member states' VAT revenues and to remove procedural requirements that would be impractical for offenses involving multiple EU MSs.

The legislation also specifies strict conditions for VAT fraud, such as executing an organized plan, involving transactions across at least two EU member states, and causing VAT losses exceeding EUR 10 million. This mirrors the PIF Directive's criteria.

Other cases of tax fraud are covered by Article 24 of Law 4689/2000 and general provisions (Article 26), which refer to various sections of the Greek Penal Code and transpose additional parts of the EU Directive. In particular, article 23 aligns with Recital 5 of the Directive, which outlines VAT offenses committed through fraudulent schemes across multiple member states. If these conditions are met, the case falls under Greek jurisdiction or the European Public Prosecutor's Office.

Offenses that do not meet these criteria are addressed by Article 66⁵⁸ of the Greek Code of Tax Procedures, which applies to broader VAT fraud cases under Greek court jurisdiction.

According to the new legislation, for the identification of the new tax crime (VAT fraud), three conditions must be met:

- the execution of an organized plan;
- the realization of transactions in the territory of at least two (2) Member States of the European Union;
- a loss of VAT resources exceeding a total of ten million (10,000,000) euros.

The above three conditions are in line with the recital of the EU Directive 2017/1371.

statements or documents or non-disclosure of information related to VAT in violation of a specific obligation to communicate them or b) presenting correct VAT related statements for the purpose of fraudulently disguising the non-payment of VAT or the illegal/wrongful creation of rights to a VAT refund, shall be punished with imprisonment of at least ten (10) years and a fine of one thousand (1000) daily units”.

⁵⁸ Article 66 of Greek Code of Tax Procedures:

“1. A tax evasion crime is committed by anyone who intentionally:

a) in order to avoid the payment of the income tax...

b) in order to avoid the payment of the VAT, the FKE, the insurance premium tax and the withheld and imposed taxes, fees or contributions, he does not pay or pays incorrectly or offsets or deducts them incorrectly, as and whoever misleads the Tax Administration by representing false facts as true or by wrongfully suppressing or concealing true facts and fails to remit or misrepresents or inaccurately sets off or deducts them or receives a refund, as well as who withholds such taxes, fees or contributions,

c) [...]

2 [...]

3. Whoever commits the crime of tax evasion referred to in paragraph 1 shall be punished by imprisonment of at least two (2) years or a fine:

a) [...]

b) if the amount to be paid of the main tax, fee or levy that was not paid or paid incorrectly or returned or set off or deducted or withheld exceeds per tax or administrative year:

aa) fifty thousand (50,000) euros, if it concerns VAT,

bb) one hundred thousand (100,000) euros per type of tax, fee or levy in any other case.

4. Imprisonment is imposed, if the amount of the tax, fee or levy referred to in paragraph 3 exceeds per fiscal or administrative year one hundred thousand (100,000) euros, if it concerns VAT, or one hundred and fifty thousand (150,000) euros in any other case of tax, fee or levy.

5 [...]

6. For the measurement of the penalty, the amount of the amount that was concealed or not returned and the duration of the concealment or non-return or inaccurate return or retention are taken into account. The treatment by the perpetrator of special tricks constitutes an aggravating circumstance”.

Also, in relation to Article 3 of the PIF Directive for criminal prosecution, Greek national legislation **prescribes specific and binding actions** in their penal codes in relation to VAT fraud, but they are the same foreseen by Article 3 of the PIF Directive.

Article 23 of Law 4689/2000 provides the following:

- by using or presenting false, incorrect/inaccurate or incomplete VAT statements or documents or non-disclosure of information related to VAT in violation of a specific obligation to communicate them;
- present correct VAT related statements to fraudulently disguise the non-payment of VAT or the illegal/wrongful creation of rights to a VAT refund.

About the subjective element, Greece provides that **only intentional acts** are punishable.

Regarding compliance with the required sanctions for the commission of fraud, described in art. 7 of the Directive, concerning Greece, the national laws do **not provide for a maximum sentence but only for a minimum sentence of 10 years for cross-border fraud**.

About compliance with **Art. 6 of the PIF Directive**, involving the liability of legal persons: **Greece amended its pre-existing legislation even if it was already adequate**. The national expert highlighted also that, while there is no specific provision for VAT fraud, with the joint provision of the crimes provided for terrorism and money laundering there could be the possibility of allowing criminal liability for legal persons (Law 4557/2018, amended by Laws 4816/2021 and 5090/2024).

About the **sanctions** as indicated in Article 9 of the PIF Directive, Greece provides:

- non-criminal fine (without specification);
- exclusion from entitlement to public benefits or aid;
- temporary or permanent exclusion from public tender procedures;
- temporary or permanent disqualification from the practice of commercial activities;
- judicial winding-up.

Greece has a **specific aggravating circumstance** related to being part of a criminal association which can be then applied to all felonies.

Finally, article 23 of Law 4689/2000 provide also as a condition for VAT fraud the execution of an organized plan, which transposes the provision of the EU Directive that “offenses are committed in a structured way”. Article 66 foresees an aggravating circumstance in the case of the execution of an organized plan.

Hungary

With respect to **compliance with Article 3 of the PIF Directive**, Hungary is compliant, having **legislation already adequate**.

Initially, in May 2022, the European Commission launched an infringement procedure against Hungary, which, however, responded by explaining why it should be considered compliant with the Directive.

The national experts highlighted that, although it is generally true that the Hungarian Criminal Code does not specifically regulate cross-border VAT fraud, the definition of “budget” under paragraph

(9) point a) of Article 396⁵⁹ includes budgets and funds managed by or on behalf of the European Union. This article, “Budget fraud” includes also activities such as the omission of facts, the

⁵⁹ Section 396 C.C.:

Budget Fraud

(1) Any person who:

a) induces a person to hold or continue to hold a false belief, or suppresses known facts in connection with any budget payment obligation or with any funds paid or payable from the budget, or makes a false statement to this extent.

b) unlawfully claims any advantage made available in connection with budget payment obligations; or

c) uses funds paid or payable from the budget for purposes other than those authorized.

and thereby causes financial loss to one or more budgets, is guilty of misdemeanor punishable by imprisonment not exceeding two years.

(2) The penalty shall be imprisonment not exceeding three years for a felony if:

a) the budget fraud results in considerable financial loss; or

b) the budget fraud defined in Subsection (1) is committed in criminal association with accomplices or on a commercial scale.

(3) The penalty shall be imprisonment between one to five years if:

a) the budget fraud results in substantial financial loss; or

b) the budget fraud results in considerable financial loss and is committed in criminal association with accomplices

or on a commercial scale.

(4) The penalty shall be imprisonment between two to eight years if:

a) the budget fraud results in particularly considerable financial loss; or

b) the budget fraud results in substantial financial loss and is committed in criminal association with accomplices

or on a commercial scale.

(5) The penalty shall be imprisonment between five to ten years if:

a) the budget fraud results in particularly substantial financial loss; or

b) the budget fraud results in particularly considerable financial loss and is committed in criminal association with

accomplices or on a commercial scale.

(6) Any person who manufactures, obtains, stores, sells or trades any excise goods in the absence of the criteria

specified in the Act on Excise Taxes and Special Regulations on the Marketing of Excise Goods or in other legislation enacted by authorization of this Act, or without an official permit, and thereby causes financial loss to the

central budget, shall be punishable in accordance with Subsections (1)-(5).

(7) Any person who either does not comply or inadequately complies with the settlement, accounting or notification obligations relating to funds paid or payable from the budget, or makes a false statement to this extent, or uses a false, counterfeit or forged document or instrument, is guilty of a felony punishable by imprisonment not

exceeding three years. (8) The penalty may be reduced without limitation if the perpetrator provides compensation for the financial loss

caused by the budget fraud referred to in Subsections (1)-(6) before the indictment is filed. This provision shall not

apply if the criminal offense is committed in criminal association with accomplices or on a commercial scale.

(9) For the purposes of this Section:

a) ‘budget’ shall mean the sub-systems of the central budget - including the budgets of social security funds and

extra-budgetary funds -, budgets and/or funds managed by or on behalf of international organizations and budgets

and/or funds managed by or on behalf of the European Union. In respect of crimes committed in connection with

funds paid or payable from a budget, ‘budget’ shall also mean - in addition to the above - budgets and/or funds

managed by or on behalf of a foreign State.

b) ‘financial loss’ shall mean any loss of revenue stemming from non-compliance with any budget payment

statement of untrue information, or obtaining improper benefits (some of the conducts indicated in Art. 3 of the PIF Directive).

VAT fraud in Hungary is classified as **a general offense (free-form)**, meaning no specific behaviors or actions are explicitly defined.

With regard to the subjective element, Hungary provides that **only intentional acts** are punishable.

Regarding compliance with the required sanctions for the commission of fraud, described in art. 7 of the Directive, **Hungary provides for a maximum sentence of 5 years of imprisonment**. But the penalty varies on the seriousness of the offense:

- for a term of one to five years if the budgetary fraud causes substantial financial loss (HUF 5 million to HUF 50 million, approximately EUR 12,500 to EUR 125,000);
- for a term of two years to eight years if the budget fraud causes particularly serious financial loss (HUF 50 million to HUF 500 million, approximately EUR 125,000 to 1,250,000);
- for a term of five to ten years if the budget fraud causes particularly serious financial loss (over HUF 500 million, approximately EUR 1,250,000).

Also, with respect to compliance with **Art. 6 of the PIF Directive**, involving the liability of legal persons, Hungary **already had compliant provisions before the Directive**.

According to national legislation, legal persons may be held liable if the offense was committed to benefit the legal person, or if the legal person was used to commit the offense. The offense must have been committed by authorized representatives, employees, or managers during the legal person's business activities. Liability may arise if the offence could have been prevented by proper management or control by the legal person's management or supervisory bodies.

Measures can also be applied if the managing director or authorized member of the legal person, or any employee or officer, was aware of the offense being committed for the benefit of the legal person.

Article 9 of the PIF Directive provides some sanctions related to legal persons. In Hungary, those are:

- up to three times the amount achieved or intended to achieve by committing the crime, but at least HUF 650'000 (approx. EUR 1,625);
- exclusion from entitlement to public benefits or aid;
- temporary or permanent exclusion from public tender procedures;
- temporary or permanent disqualification from the practice of commercial activities;
- judicial winding-up.

Finally, Hungary foresees the possibility of applying an **aggravating circumstance** in cases where organised groups are involved.

obligation, as well as the claiming of funds from a budget unlawfully or the use of funds paid or payable from a budget for purposes other than those authorized.

Ireland

With respect to **compliance with Article 3 of the PIF Directive** Ireland is compliant by amendment of pre-existing discipline.

The relevant legislative references are: Section 42⁶⁰, Criminal Justice (Theft and Fraud Offences) Act, as amended by Section 3, Section 40⁶¹, Criminal Justice (Theft and Fraud Offences) Act, as amended by Section 2, Criminal Justice (Theft and Fraud Offences) (Amendment) Act 2021.

In Ireland, **VAT fraud is classified as a general offense (free-form)**, meaning no specific behaviors or actions are explicitly defined.

About the subjective element, Ireland provides that **only intentional acts** are punishable.

Ireland is compliant with Art. 7 of the PIF Directive, having a maximum sentence of **5 years of imprisonment** in cases where the fraud committed against the financial interests of the EU had led to a damage of over 100.000 € (threshold established for the “considerable damage”).

The **liability of legal persons** was foreseen by the introduction of new legislation. The relevant legal reference is Section 42 B⁶², of Criminal Justice (Theft and Fraud Offences) Act 2001 Act, inserted by Section 7 of Criminal Justice (Theft and Fraud Offences), (Amendment) Act 2021.

⁶⁰ 42(1) - Subject to subsection (2), a person who intentionally commits any fraud affecting the financial interests of the European Union is guilty of an offence and is liable on conviction on indictment to a fine or to imprisonment for a term not exceeding 5 years or both.

42(2) - Where an offence under subsection (1) relates to acts or omissions to which Article 3(2)(d) of the Directive applies, the offence is not committed unless such acts or omissions are connected with the territory of two or more Member States and involve a total damage of not less than €10,000,000.

⁶¹ 40(1) – In this part [...]

"Directive" means Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, the text of which is, for convenience of reference, set out in Schedule 1A.

"Fraud affecting the financial interests of the European Union" has the same meaning as "fraud affecting the Union's financial interests" in Article 3(2) of the Directive.

⁶² 42B of Criminal Justice (Theft and Fraud Offences) Act

(1) Where a relevant offence is committed for the benefit of a body corporate by a relevant person and the commission of the relevant offence is attributable to the failure, by a director, manager, secretary or other officer of the body corporate, or a person purporting to act in that capacity, to exercise, at the time of the commission of the relevant offence and in all the circumstances of the case, the requisite degree of supervision or control of the relevant person, the body corporate shall be guilty of an offence.

(2) In proceedings for an offence under subsection (1), it shall be a defense for a body corporate against which such proceedings are brought to prove that it took all reasonable steps and exercised all due diligence to avoid the commission of the offence.

(3) Where an offence under section 42 or 42A, or an offence of inciting, aiding and abetting, or attempting the commission of such an offence, is committed by a body corporate and it is proved that the offence was committed with the consent or connivance, or was attributable to any willful neglect, of a person who was a director, manager, secretary or other officer of the body corporate, or a person purporting to act in that capacity, that person shall, as well as the body corporate, be guilty of an offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.

(4) Where the affairs of a body corporate are managed by its members, subsection (3) shall apply in relation to the acts and defaults of a member in connection with his or her functions of management as if he or she were a director or manager of the body corporate.

(5) Subsection (1)–

(a) is without prejudice to the other circumstances, under the general law, whereby acts or omissions of a natural person are attributed to a body corporate resulting in criminal liability of that body corporate for those acts or omissions, and

The sanctions foreseen are:

- criminal fine (no specification available);
- non-criminal fine (no specification available);
- exclusion from entitlement to public benefits or aid;
- temporary or permanent exclusion from public tender procedures;
- temporary or permanent disqualification from the practice of commercial activities;
- placing under judicial supervision;
- judicial winding-up;
- temporary or permanent closure of establishments that have been used for committing the criminal offense.

Ireland provides for an **aggravating circumstance** if the offense is committed within the framework of an organized criminal group, under the Criminal Justice (Organised Crime) Act 2006.

Italy

Italy is compliant with **Article 3 of the PIF Directive. To be compliant**, Italy amended its pre-existing discipline. The PIF Directive was transposed into Italian law by Law No. 3 of January 9, 2020, which amended the Penal Code and Legislative Decree No. 74/2000 (on tax crimes). Specifically, the amendments were about these legal references: Art. 316 ter⁶³ (undue receipt of public funds) and

(b) does not exclude criminal proceedings against natural persons who are involved as perpetrators, inciters or accessories in an offence referred to in that subsection.

(6) A person guilty of an offence under subsection (1) is liable on conviction on indictment to a fine.

(7) In this section—

"Relevant person", in relation to a body corporate, means—

(a) a director, manager, secretary or other officer of the body corporate, or a person purporting to act in that capacity, or

(b) an employee, subsidiary or agent of the body corporate.

"relevant offence" means:

(a) an offence under section 42 or 42A,

(b) a money laundering offence involving property derived from the proceeds of an offence referred to in paragraph (a), (c) or (d),

(c) a corruption offence that damages, or is likely to damage, the financial interests of the European Union, or

(d) an offence of inciting, aiding and abetting, or attempting the commission of an offence referred to in paragraph (a), (b) or (c).

"subsidiary", in relation to a body corporate, has the same meaning as it has in the Companies Act 2014.

⁶³ Art. 316 ter C.C.:

(Modified by art. 3, c. 1, lett. f) Law n. 117/2019 – following PIF)

Unless the fact constitutes the crime provided for by article 640 bis, anyone who, through the use or presentation of false declarations or documents or attesting to untrue things, or through the omission of required information, unduly obtains, for himself or for others, contributions, grants, loans, subsidized mortgages or other disbursements of the same type, however named, granted or disbursed by the State, other public bodies or the European Communities is punished with imprisonment from six months to three years. The penalty is imprisonment from one to four years if the act is committed by a public official or by a person in charge of a public service with abuse of his capacity or powers. The penalty is imprisonment from six months to four years if the act offends the financial interests of the European Union and the damage or profit exceeds 100,000 euros. When the sum unduly received is equal to or less than €3,999.96, only the administrative sanction of paying a sum of money from €5,164 to €25,822 is applied. However, this penalty cannot exceed three times the benefit achieved.

640⁶⁴ (fraud) Italian Criminal Code and Art. 2⁶⁵ (fiscal fraud), 3⁶⁶ (failure to file a declaration), 4⁶⁷ (falsification or use of false documents) D. lgs. 74/2000 as amended by D. lgs. 75/2020 and D. lgs. 156/2022.

⁶⁴ Art. 640 C.C.:

Anyone who, through artifice or deception, misleading someone, procures for himself or others an unfair profit to the detriment of others, is punished with imprisonment from six months to three years and with a fine ranging from 51 euros to 1,032 euros.

The penalty is imprisonment from one to five years and a fine from €309 to €1,549:

1) if the act is committed to the detriment of the State or another public body or of the European Union or with the pretext of exempting someone from military service.

2) if the act is committed generating in the offended person the fear of an imaginary danger or the erroneous belief of having to carry out an order from the Authority.

2-bis) if the act is committed in the presence of the circumstance referred to in article 61, number 5.

2-ter) if the act is committed remotely through IT or telematic tools capable of hindering one's own or others' identification.

The crime is punishable upon complaint by the offended person, unless some of the circumstances provided for in the second paragraph apply, with the exception of that referred to in number 2-ter).

⁶⁵ Art. 2 D. lgs. 74/2000:

1. Anyone who, in order to evade income or value added taxes, using invoices or other documents for non-existent transactions, indicates fictitious passive elements in one of the declarations relating to said taxes, is punished with imprisonment from four to eight years.

2. The act is considered to have been committed by making use of invoices or other documents for non-existent transactions when such invoices or documents are recorded in the mandatory accounting records or are held for the purpose of proof against the financial administration.

2-bis. If the amount of the fictitious passive elements is less than one hundred thousand euros, imprisonment from one year and six months to six years is applied.

⁶⁶ Art. 3 D. lgs. 74/2000:

1. Except for cases provided for in article 2, anyone who, with the aim of evading income or value added taxes, carries out objectively or subjectively simulated operations or makes use of false documents or other fraudulent means capable of hindering the assessment and misleading the financial administration, indicates in one of the declarations relating to said taxes active elements for an amount lower than the actual one or fictitious passive elements or fictitious credits and withholdings, when, jointly:

a) the tax evaded is greater, with reference to some of the individual taxes, than thirty thousand euros.

b) the total amount of the active elements subtracted from taxation, also through the indication of fictitious passive elements, is greater than five percent of the total amount of the active elements indicated in the declaration, or in any case, is greater than one million five hundred thousand euros, or if the total amount of credits and fictitious withholdings reducing the tax is greater than five percent of the amount of the tax itself or in any case more than thirty thousand euros.

2. The act is considered to have been committed using false documents when such documents are recorded in the mandatory accounting records or are held for the purposes of proof against the financial administration.

3. For the purposes of applying the provision of paragraph 1, the mere violation of the invoicing and annotation obligations of the active elements in the accounting records or the sole indication in the invoices or annotations of active elements that are lower than the real ones do not constitute fraudulent means.

⁶⁷ Art. 4 D. lgs. 74/2000:

1. Except for cases provided for in articles 2 and 3, anyone who, in order to evade income or value added taxes, indicates in one of the annual declarations relating to said taxes active elements for an amount lower than the actual amount or non-existent passive elements, when jointly:

a) the tax evaded is greater, with reference to some of the individual taxes, than one hundred thousand euros.

b) the total amount of the active elements subtracted from taxation, also through the indication of non-existent passive elements, is greater than ten percent of the total amount of the active elements indicated in the declaration, or, in any case, is greater than two million euros.

1-bis. For the purposes of applying the provision of paragraph 1, incorrect classification and the evaluation of objectively existing active or passive elements are not taken into account, with respect to which the criteria actually applied have in any case been indicated in the financial statements or in other documentation relevant for the purposes tax, the violation of the criteria for determining the relevant financial year, the non-inherence, the non-deductibility of real passive elements.

Article 640 bis⁶⁸, which concerns fraud to the detriment of the State or a public entity, and provides penalties for those who, through deceit or tricks, unlawfully obtain public funds or avoid payment of amounts due to the State, can also be seen as one of the tools used in Italy to implement the obligations arising from the PIF Directive, even though it does not explicitly refer to it. The PIF Directive promotes cooperation among Member States and coordinated action to combat financial fraud, and Article 640-bis is one of the provisions that allows the Italian legal system to comply with these obligations.

In relation to the conducts foreseen by Article 3 of the PIF Directive for criminal prosecution, Italian national legislation covers all of them.

About the subjective element, Italy provides that **only intentional acts** are punishable.

Italy is compliant with Article 7 of the Directive having a maximum sentence of at least **8 years of imprisonment** in cases where the fraud committed against the financial interests of the EU had led to damage of over 100.000 € (threshold established for the “considerable damage”), and up to 6 years when the damage is lower than the threshold.

Italian legislation has been amended to include the specific responsibility of legal entities in cases of VAT fraud and frauds involving EU funds (Article 7 of Legislative Decree 74/2000) to be compliant with Art. **6 of the PIF Directive**. However, in general, the administrative liability of legal entities for crimes is regulated by Legislative Decree 231/2001.

About **sanctions** indicated in Article 9 of the PIF Directive, the relevant legal reference is Article 25 quinquies decies⁶⁹ D.lgs.231/2001.

1-ter. Except for the cases referred to in paragraph 1-bis, assessments which, taken as a whole, differ by less than 10 percent from the correct ones do not give rise to punishable offences.
The amounts included in this percentage are not taken into account when verifying whether the criminality thresholds set out in paragraph 1, letters a) and b) have been exceeded.”

⁶⁸ Art. 640bis C.C.:

The penalty is imprisonment from two to seven years and action is taken automatically if the fact referred to in article 640 concerns contributions, grants, loans, subsidized mortgages or other disbursements of the same type, however named, granted or disbursed by the State, other public bodies or the European Communities.

⁶⁹ Art. 25-quinquies decies D.lgs. 231/2001:

1. In relation to the commission of the crimes envisaged by the legislative decree of 10 March 2000, n. 74, the following financial sanctions apply to the entity:

- a) for the crime of fraudulent declaration through the use of invoices or other documents for non-existent transactions provided for in article 2, paragraph 1, a financial penalty of up to five hundred quotas.
- b) for the crime of fraudulent declaration through the use of invoices or other documents for non-existent transactions, provided for in article 2, paragraph 2-bis, a financial penalty of up to four hundred quotas.
- c) for the crime of fraudulent declaration through other devices, provided for in article 3, a financial penalty of up to five hundred quotas.
- d) for the crime of issuing invoices or other documents for non-existent operations, provided for in article 8, paragraph 1, a financial penalty of up to five hundred quotas.
- e) for the crime of issuing invoices or other documents for non-existent transactions, provided for in article 8, paragraph 2-bis, a financial penalty of up to four hundred quotas.
- f) for the crime of concealment or destruction of accounting documents, provided for in article 10, a financial penalty of up to four hundred quotas.
- g) for the crime of fraudulent evasion of the payment of taxes, provided for in article 11, a pecuniary sanction of up to four hundred quotas.

1-bis. In relation to the commission of the crimes foreseen by the legislative decree of 10 March 2000, n. 74, when they are committed with the aim of evading value added tax as part of cross-border fraudulent systems connected to the territory of at least one other Member State of the European Union, which results or may result in overall damage equal to or greater than ten million euros, the following financial sanctions apply to the entity:

Italy has an **aggravating circumstance** in the case of VAT fraud committed by organized criminal groups. Indeed, under Law No. 146/2006, "Ratification and implementation of the United Nations Convention and Protocols against Transnational Organized Crime, adopted by the General Assembly on November 15, 2000, and May 31, 2001," all crimes committed within the framework of an organized criminal group are subject to more severe penalties.

Latvia

Regarding **compliance with Article 3** of the PIF Directive, Latvia initially faced an infringement procedure initiated by the European Commission in December 2021. However, Latvia has since taken corrective action, specifically with **new legislative provisions**, and is now fully compliant with both the PIF Directive and Article 3.

In particular, the compliance was possible thanks to the new Section 218.1⁷⁰ of the Criminal Law (CL) titled "Recording of a Fictitious Transaction in a Value Added Tax (VAT) Declaration", which came into force on August 5, 2021. It encompasses both VAT evasion and fraudulent claims for

a) for the crime of unfaithful declaration provided for in article 4, a financial penalty of up to three hundred quotas.

b) for the crime of failure to declare provided for in article 5, a pecuniary sanction of up to four hundred quotas.

c) for the crime of undue compensation provided for in article 10 quater, a pecuniary sanction of up to four hundred quotas.

2. If, following the commission of the crimes indicated in paragraphs 1 and 1-bis, the entity has achieved a significant profit, the pecuniary sanction is increased by one third.

3. In the cases provided for in paragraphs 1, 1-bis and 2, the disqualification sanctions referred to in article 9, paragraph 2, letters c), d) and e) shall apply.

⁷⁰ **Article 218.1 C.C.:**

Indication of a Transaction that Has not Actually Occurred in the Value Added Tax Return

(1) For a person who commits the indication in the value added tax return of a transaction taxable with value added tax which has not actually occurred, if the total value of the transaction indicated in the return and not having occurred or of several such transactions reaches a large amount, the applicable punishment is the deprivation of liberty for a period of up to two years or temporary deprivation of liberty, or community service, or fine.

(2) For a person who commits the indication in the value added tax return or in several such returns of a transaction taxable with value added tax which has not actually occurred, if losses have been caused thereby to the State on a significant scale, the applicable punishment is the deprivation of liberty for a period of up to five years or temporary deprivation of liberty, or community service, or fine, with deprivation of the right to engage in entrepreneurial activity of a specific type or of all types or to a specific employment, or the right to take up a specific office for a period of two years and up to five years.

(3) For a person who commits the acts provided for in Paragraph two of this Section, if losses have been caused thereby to the State on a significant scale, or for the criminal offence provided for in Paragraph one or two of this Section, if it has been committed by an organised group, the applicable punishment is the deprivation of liberty for a period of up to ten years, with or without confiscation of property and with deprivation of the right to engage in entrepreneurial activity of a specific type or of all types or to a specific employment, or the right to take up a specific office for a period of two years and up to five years, and with probationary supervision for a period of up to three years.

VAT refunds. Additionally, Sections 177⁷¹ (fraud), 217⁷² (Violation of provisions regarding accounting and statistical information for a person who commits hiding or forging of accounting documents), 218⁷³ (Evasion of tax payments and payments equivalent thereto), 195.1⁷⁴ (Non-

⁷¹ Section 177 C.C.:

Fraud

(1) For a person who commits acquiring property of another, or of rights to such property, by the use, in bad faith, of trust, or by deceit (fraud),

the applicable punishment is the deprivation of liberty for a period of up to three years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

(2) For a person who commits fraud if it has been committed on a significant scale or if it has been committed by a group of persons according to a prior agreement, the applicable punishment is the deprivation of liberty for a period of up to five years or temporary deprivation of liberty, or probationary supervision, or community service, or fine, with or without confiscation of property.

(3) For a person who commits fraud, if it has been committed on a large scale, or it has been committed by an organised group, or it has been committed, acquiring narcotic, psychotropic, powerfully acting, poisonous or radioactive substances or explosive substances, firearms or ammunition, the applicable punishment is the deprivation of liberty for a period of two years and up to ten years, with or without confiscation of property and with or without probationary supervision for a period of up to three years.

⁷² Section 217 C.C.:

Violation of Provisions Regarding Accounting and Statistical Information

(1) For a person who commits hiding or forging of accounting documents, annual accounts, statistical reports or statistical information specified in the law for an undertaking (company), institution or organisation, the applicable punishment is the deprivation of liberty for a period of up to one year or temporary deprivation of liberty, or community service, or fine.

(2) For the commission of the same acts if they have caused substantial harm, the applicable punishment is the deprivation of liberty for a period of up to four years or temporary deprivation of liberty, or community service, or fine. (3) For a person who commits the criminal offence provided for in Paragraph two of this Section, if it has been committed for acquiring property, the applicable punishment is the deprivation of liberty for a period of up to five years or temporary deprivation of liberty, or community service, or fine.

⁷³ Section 218 C.C.:

Evasion of Tax Payments and Payments Equivalent Thereto

(1) [13 December 2012]

(2) For a person who commits evasion of tax payments and payments equivalent thereto or of concealing or reducing income, profits and other items subject to tax, if losses on a large scale are caused thereby to the State or local government,

the applicable punishment is the deprivation of liberty for a period of up to four years or temporary deprivation of liberty, or community service, or fine, with or without confiscation of property and with deprivation of the right to engage in entrepreneurial activity of a specific type or of all types or to a specific employment,

or the right to take up a specific office for a period of two years and up to five years.

(3) For the criminal offence provided for in Paragraph two of this Section, if it has been committed by an organised group,

the applicable punishment is the deprivation of liberty for a period of up to ten years, with or without confiscation of property and with deprivation of the right to engage in entrepreneurial activity of a specific type or of all types or to a specific employment, or the right to take up a specific office for a period of two years and

up to five years, and with probationary supervision for a period of up to three years.

⁷⁴ Section 195.1 C.C.:

Non-provision of Information and Provision of False Information Regarding Ownership of Resources and the True Beneficiary

(1) For a person who knowingly commits provision of false information to a natural or legal person which is authorised by law to request information regarding a transaction and the true owner and true beneficiary of the financial resources or other property involved therein, as well as non-provision of the information specified in the law regarding the true beneficiary or provision of knowingly false information to a state institution or legal person, the applicable punishment is the deprivation of liberty for a period of up to one year or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

provision of information and provision of false information regarding ownership of resources and the real beneficiary), 300⁷⁵ (Knowingly giving false testimony, opinion, translation, explanation, and application), 302⁷⁶ (Refusal to give testimony or opinions, or provide translations), and 328⁷⁷ (False official information) of the Criminal Law align with Article 3 of Directive 2017/1371, covering various tax fraud and false information provisions related to EU and national revenues, including violations of accounting rules, providing false information to state institutions, and failing to submit accurate declarations.

If none of the relevant criminal sections apply, Section 3 of the Administrative Procedure Law establishes administrative liability for failing to provide or provide false information.

VAT fraud is classified as a general offense (free-form), meaning no specific behaviors or actions are explicitly defined.

About the subjective element, Latvia provides that **only intentional acts** are punishable.

Latvia is compliant also with **Article 7, on sanctions**, having a maximum sentence of **at least 4 years of imprisonment** in cases where the fraud committed against financial interests of the EU had led to damage over 100.000 € (threshold established for the “considerable damage”).

(2) For the commission of the same acts, if substantial harm has been caused thereby, the applicable punishment is the deprivation of liberty for a period of up to two years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

⁷⁵ Section 300 C.C.:

Knowingly Giving a False Testimony, Opinion, Translation, Explanation and Application

(1) For a person who knowingly gives a false testimony, opinion, translation, explanation or application during administrative offence proceedings in an institution, during pre-trial criminal proceedings, in court, to a notary or bailiff, if it has been committed by a person who has been warned about criminal liability for knowingly giving a false testimony, opinion, translation, explanation or application, the applicable punishment is the temporary deprivation of liberty or probationary supervision, or community service, or fine.

(2) For the commission of the same acts, if they have been committed during performance of pre-trial criminal proceedings or trial in court of matters concerning serious or especially serious crimes, or serious consequences result therefrom, or they have been committed for the purpose of acquiring property, the applicable punishment is the deprivation of liberty for a period of up to three years or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

⁷⁶ Section 302 C.C.:

Refusal to Give Testimony or Opinions, or Provide Translations

(1) For a person who, being a witness, a victim or another person who has been warned against refusal to give testimony, commits unfounded refusal to give testimony in administrative offence proceedings in an institution, in a pre-trial investigating institution, the Office of the Prosecutor or at a trial, the applicable punishment is the temporary deprivation of liberty or probationary supervision, or community service, or fine.

(2) For a person who, being an expert or translator, commits unfounded refusal to perform the tasks assigned to him or her in administrative offence proceedings in an institution, in a pre-trial investigating institution, the Office of the Prosecutor or at a trial, the applicable punishment is the temporary deprivation of liberty or probationary supervision, or community service, or fine.

⁷⁷ Section 328 C.C.:

False Official Information

For a person who knowingly commits providing false information to an institution or a public official who has the right to request such information, or commits concealing or knowingly failing to inform of a document or information, if it has been committed by a public official whose responsibilities include the providing of such information, and substantial harm has been caused thereby, the applicable punishment is the deprivation of liberty for a period of up to one year or temporary deprivation of liberty, or probationary supervision, or community service, or fine.

With respect to compliance with Art. 6 of the PIF Directive, involving the **liability of legal persons**, Latvia already had compliant provisions before the Directive (Art.70.1⁷⁸ and Art.70.2⁷⁹ of the Criminal Law of Latvia).

About sanctions as indicated in Article 9 of the PIF Directive, article 70.2 in footnotes provides:

- 1) criminal fine for a criminal violation - in the amount of five and up to ten thousand minimum monthly wages;
- 2) for a less serious crime - in the amount of ten and up to fifty thousand minimum monthly wages;
- 3) for a serious crime - in the amount of twenty and up to seventy-five thousand minimum monthly wages;
- 4) for an especially serious crime - in the amount of thirty and up to a hundred thousand minimum monthly wages);
- 5) exclusion from entitlement to public benefits or aid;
- 6) temporary or permanent exclusion from public tender procedures;
- 7) temporary or permanent disqualification from the practice of commercial activities;
- 8) judicial winding-up.

Latvia has an **aggravating circumstance** for VAT fraud committed by organised criminal groups, according to Article 8 of PIF Directive.

⁷⁸ Section 70.1 C.C.:

Basis for the Application of a Coercive Measure to a Legal Person

For the criminal offences provided for in the Special Part of this Law, a court or in the cases provided for by the Law - a prosecutor may apply a coercive measure to a legal person governed by private law, including State or local government capital company, as well as partnership, if a natural person has committed the offence in the interests of the legal person, for the benefit of the person or as a result of insufficient supervision or control, acting individually or as a member of the collegial authority of the relevant legal person:

- 1) on the basis of the right to represent the legal person or act on the behalf thereof; 2) on the basis of the right to take a decision on behalf of the legal person.
- 3) in implementing control within the scope of the legal person.

⁷⁹ Section 70.2 C.C.:

Types of Coercive Measures Applicable to a Legal Person

(1) For a legal person one of the following coercive measures may be specified:

- 1) liquidation.
- 2) restriction of rights.
- 3) confiscation of property,
- 4) recovery of money.

(2) For a legal person one or several of the coercive measures provided for in Paragraph one of this Section may be applied. In applying liquidation, other coercive measures shall not be specified.

(3) The procedures for executing coercive measures shall be determined in accordance with the law.

(4) For a criminal violation, a less serious crime or a serious crime for which deprivation of liberty for a period of up to five years is provided for in the Special Part of this Law a prosecutor, in drawing up a penal order regarding the coercive measure, may determine the recovery of money or restriction of rights as a coercive measure to a legal person.

Lithuania

Concerning compliance with Article 3 of the PIF Directive Lithuania is compliant, by amendment of a pre-existing discipline. The relevant legal provisions are Articles 182⁸⁰ (Fraud), 183⁸¹ (Misappropriation), 205⁸² (Misleading declarations), 206⁸³ (Misuse of use of credit, loan or

⁸⁰ Article 182 C.C.:

Fraud

1. A person who, by deceit, acquires another's property for own benefit or for the benefit of other persons or acquires a property right, avoids a property obligation or annuls it, shall be punished by community service or by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to three years.
2. A person who, by deceit and for own benefit or for the benefit of other persons, acquires another's property of a high value, shall be punished by a fine, or restriction of liberty, or by arrest, or custodial sentence for a term of up to six years.
3. A person who, by deceit and for own benefit or for the benefit of other persons, acquires another's property of a very high value, or a property right or the valuables of a considerable scientific, historical or cultural significance or avoids a property obligation of a very high value or annuls it or swindles by participating in an organised group, shall be punished by a custodial sentence for a term of up to eight years.
4. A person who, by deceit and for own benefit or for the benefit of other persons, acquires another's property of a low value or acquires a property right, avoids a property obligation of a low value or annuls it shall be considered to have committed a misdemeanor and shall be punished by community service or by a fine or by restriction of liberty or by arrest.
5. A person shall be held liable for the acts provided for in paragraphs 1 and 4 of this Article only under a complaint filed by the victim or a statement by the legal representative thereof or at the prosecutor's request.
6. Legal entities shall also be held liable for the acts provided for in paragraphs 1, 2 and 3 of this Article.

⁸¹ Article 183 C.C.:

Misappropriation of Property

1. A person who misappropriates another's property or property right entrusted to him or held at his disposal shall be punished by community service or by a fine or by a custodial service for a term of up to three years.
2. A person who misappropriates another's property or property right of a high value entrusted to him, shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to six years.
3. A person who misappropriates another's property or property right of a very high value entrusted to him or held at his disposal or the valuables of a considerable scientific, historical or cultural significance, shall be punished by a fine or by a custodial sentence for a term of up to eight years.
4. A person who misappropriates another's property or property right of a low value entrusted to him or held at his disposal shall be considered to have committed a misdemeanor and shall be punished by community service or by a fine or by arrest.
5. Legal entities shall also be held liable for the acts provided for in paragraphs 1, 2 and 3 of this Article.
6. A person shall be held liable for the acts provided for in paragraphs 1 and 4 of this Article only under a complaint filed by the victim or a statement by the legal representative thereof or at the prosecutor's request.

⁸² Article 205 C.C.:

Misleading Declaration about the Activities of a Legal Entity

1. A person who, on behalf of a legal entity, presents in an official report or in an application misleading data concerning the activities or assets of the legal entity and thereby misleads a State or European Union institution, international public organisation, creditor, member of the legal entity or another person who suffers major material damage as a result thereof, shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to four years.
2. A legal entity shall also be held liable for an act provided for in this Article.

⁸³ Article 206 C.C.:

Use of a Credit, Loan or Targeted Support Not in Accordance with Its Purpose or the Established Procedure

1. A person who, upon obtaining a credit, loan or targeted support in the amount of 400 MSLS or more, uses it not in accordance with its purpose or the established procedure, shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to one year.
2. A person who, upon obtaining a credit or loan, uses it not in accordance with its purpose or the established procedure and fails to repay it within the established time limit thereby incurring large material damage to

targeted support), 207⁸⁴ (credit fraud), 220⁸⁵ (Provision of inaccurate data on income, profit or assets), 221⁸⁶ (Failure to file a tax return or to submit a report or another document), 222⁸⁷

the creditor, guarantor or another person, shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to four years.

3. A person who obtains targeted support, subsidy or grant, uses it not in accordance with its purpose or the established procedure and as a result caused large material damage to a State or European Union institution, an international public organization or another legal or natural person, shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to six years.

4. A person who obtains targeted support, subsidy or grant, uses it not in accordance with its purpose or the established procedure and as a result caused very large material damage to a State or European Union institution, an international public organization or another legal or natural person, or committed an act by participating in an organized group, shall be punished by a fine or by a custodial sentence for a term of up to seven years.

5. A legal entity shall also be held liable for the acts provided for in this Article.

⁸⁴ Article 207 C.C.:

Credit Fraud

1. A person who, by deceit, obtains a credit, loan, subsidy, warranty or bank guarantee statement or another credit obligation, shall be punished by a fine or by arrest or by a custodial sentence for a term of up to three years.

2. A person who, by deceit, obtains targeted support, subsidy or grant and as a result caused large material damage to a State or European Union institution, an international public organization or another legal or natural person, shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to six years.

3. A person who, by deceit, obtains targeted support, subsidy or grant and as a result caused very large material damage to a State or European Union institution, an international public organization or another legal or natural person, or committed an act by participating in an organized group, shall be punished by a fine or by a custodial sentence for a term of up to eight years.

4. A legal entity shall also be held liable for an act provided for in this Article.

⁸⁵ Article 220 C.C.:

Provision of Inaccurate Data on Income, Profit or Assets

1. A person who, seeking to evade the payment of taxes the amount whereof exceeds 400 MSLs, provides data on the person's income, profit, assets or the use thereof that are known to be inaccurate in a tax return or in a report approved in accordance with the specified procedure or in another document and submits such data to an institution authorised by the State shall be punished by a fine or by a custodial sentence for a term of up to four years.

2. A person who commits the act indicated in paragraph 1 of this Article, where the tax amount exceeds 900 MSLs or by participating in an organised group, shall be punished by a custodial sentence for a term of up to eight years.

3. A legal entity shall also be held liable for the acts provided for in this Article.

⁸⁶ Article 221 C.C.:

Failure to File a Tax Return or to Submit a Report or Another Document

1. A person who fails, in accordance with the procedure laid down by legal acts and seeking to evade the payment of taxes or other fees the amount whereof exceeds 400 MSLs, to timely file with an institution authorised by the State a tax return or to submit thereto a report approved in accordance with the specified procedure or another document concerning a person's income, profit or assets after this state institution reminds him in writing of the duty to submit them, shall be punished by a fine or by a custodial sentence for a term of up to four years.

2. A person who commits the act indicated in paragraph 1 of this Article, where the amount of taxes or other fees exceeds 900 MSLs, shall be punished by a custodial sentence for a term of two up to seven years.

3. A legal entity shall also be held liable for the acts provided for in this Article.

⁸⁷ Article 222 C.C.:

Fraudulent Management of Accounts

1. A person who fraudulently manages and (or) organizes the financial accounts required by legal acts or did not keep financial accounting documents and (or) financial accounting registers for the period prescribed by law, or conceals, destroys or damages financial accounting documents and (or) financial accounting registers, or did not manage and (or) did not organize the financial accounting required by legislation, if this resulted in large material damage to the State or a natural or legal person, or where this disables, fully or in

(Fraudulent management of accounts) and 228⁸⁸ (Abuse of office) of the Criminal Code of Lithuania).

VAT fraud is classified as a **general offense (free-form)**, meaning no specific behaviors or actions are explicitly defined.

About the subjective element, Lithuania provides that **only intentional acts** are punishable.

In relation to compliance with the sanctions for committing fraud, described in Article 7 of the Directive, Lithuania complies, providing for a maximum penalty of **8 years imprisonment** in cases where the fraud committed against the EU's financial interests had caused damage exceeding EUR 100,000 (the threshold for “considerable damage”). In the variety of offenses that may come into play, the penalties vary significantly, ranging from 4 to 7 to 8 years.

Regarding **compliance with Article 6** of the PIF Directive, which addresses the liability of legal persons, Lithuania had already established compliant provisions before the adoption of the Directive (Article 20 of the C.C.⁸⁹).

part, determination of the person's activities, the amount or structure of the assets, equity or liabilities thereof, shall be punished by a fine or by arrest or by a custodial sentence for a term of up to four years.

2. The person who committed the act provided for in paragraph 1 of this article by causing very large material damage to the State or to a natural or legal person, shall be punished by a fine by a custodial sentence for a term of up to seven years.

3. A legal entity shall also be held liable for the acts provided for in this Article.

⁸⁸ Article 228 C.C.:

Abuse of Office

1. A civil servant or a person equivalent thereto who abuses his official position or exceeds his powers, where this incurs major damage to the State, the European Union, an international public organisation, a legal or natural person, shall be punished by a fine or by arrest or by a custodial sentence for a term of up to five years.

2. A person who commits the act provided for in paragraph 1 of this Article seeking material or another personal gain, in the absence of characteristics of bribery, shall be punished by a fine or a custodial sentence for a term of up to seven years.

3. A legal entity shall also be held liable for the acts provided for in this Article.

⁸⁹ Article 20 C.C.:

Criminal Liability of a Legal Entity

1. A legal entity shall be held liable solely for the criminal acts the commission whereof is subject to liability of a legal entity as provided for in the Special Part of this Code.

2. A legal entity shall be held liable for the criminal acts committed by a natural person solely where a criminal act was committed for the benefit or in the interests of the legal entity by a natural person acting independently or on behalf of the legal entity, provided that he, while occupying an executive position in the legal entity, was entitled:

- 1) to represent the legal entity, or
- 2) to take decisions on behalf of the legal entity, or
- 3) to control activities of the legal entity.

3. A legal entity may be held liable for criminal acts also where they have been committed by an employee or authorised representative of the legal entity on the instruction or with the permission of or as a result of insufficient supervision or control by the person indicated in paragraph 2 of this Article.

4. A legal entity may be held liable for the criminal acts committed under the conditions indicated in paragraph 2 or 3 of this Article by another legal entity controlled by or representing it, where they have been committed for the benefit of the abovementioned legal entity on the instruction or with the permission of or as a result of insufficient supervision or control by a person holding a management position therein or a person authorised by him.

5. The criminal liability of a legal entity shall not release from criminal liability a natural person who has committed, organised, instigated or assisted in commission of a criminal act. The criminal liability of a legal entity for a criminal act committed, organised, instigated or assisted in by a natural person for the benefit or in the interests of the legal entity shall not be released by the criminal liability of the natural person, nor by

In Lithuania, sanctions applicable to legal persons (according to Article 9 of the PIF Directive) are fines, ranging from a minimum of 200 BAPPs (basic amount of punishments and penalties) to a maximum of 100,000 BAPPs. As per the Government's decision, effective since January 1, 2018, one BAPP is equivalent to EUR 50.

Lithuania has an **aggravating circumstance** for the VAT fraud committed by organised criminal groups, according to Article 8 of PIF Directive.

Luxembourg

In relation to compliance with Article 3 of the PIF Directive, which concerns the criminalisation of the commission of fraud against the EU's financial interests, Luxembourg is **compliant** having indeed **amended a pre-existing discipline**, specifically Art. 496-4⁹⁰ (budgetary fraud) and 501⁹¹ (offenses against the integrity of financial instruments) Luxembourgian Criminal Code as amended by l. 12 March 2020.

VAT fraud in Luxembourg is classified as a **general offense (free-form)**, meaning no specific behaviors or actions are explicitly defined

About the subjective element, Luxembourg provides that **only intentional acts** are punishable.

In relation to compliance with the sanctions for committing fraud, described in Article 7 of the Directive, Luxemburg complies, providing for a **maximum penalty of 4 years imprisonment** in cases where the fraud committed against the EU's financial interests had caused damage exceeding EUR 100,000 (the threshold for “considerable damage”)⁹².

the fact that the natural person is released from criminal liability for this act or is not held liable for other reasons.

6. The State, a municipality, a state and municipal institution and agency as well as an international public organisation shall not be held liable under this Code. The state and municipal enterprises, also the public establishments whose owner or stakeholder the State or a municipality, also the public limited liability companies and private limited liability companies whose shares, in whole or in part, belong by the right of ownership to the State or the municipality shall not be considered as state and municipal institutions and agencies and shall be held liable under this Code.

⁹⁰ Art. 496-4 C.C.:

Anyone who knowingly makes a false or incomplete declaration or fails to disclose information in violation of a specific obligation, with the intent to evade or reduce their legal contribution to the resources of an international institution's budget or the budgets managed by the European Union or on its behalf, shall be subject to the penalties provided under Article 496.

(As amended by the Law of July 29, 2022) The same penalties apply to anyone who knowingly misappropriates a legally obtained benefit and unlawfully reduces the resources of an international institution's budget or the budgets managed by the European Union or on its behalf.

⁹¹ Art. 501 C.C.:

Shall be punished with imprisonment of eight days to one year and a fine of 251 euros to 10,000 euros, or with only one of these penalties, those who, even without fraudulent intent, have manufactured, sold, peddled, or distributed any objects, instruments, prints, or templates obtained by any process which, due to their external appearance, resemble currency, government bonds, postage or telegraph stamps, securities representing ownership rights, claims, or financial instruments (other than monetary signs in the form of banknotes), or in general, fiduciary instruments issued in the Grand Duchy or abroad, in a manner likely to facilitate the acceptance of said objects, instruments, prints, or templates in place of the imitated values. (Amended by the law of January 13, 2002) The objects, instruments, prints, or templates, as well as the plates or matrices used for their production, shall also be confiscated, even if they are not the property of the convicted person.

⁹² Article 80 §1 Luxembourg VAT legislation.

With respect to compliance with Article 6 of the PIF Directive, concerning the liability of legal persons, **Luxembourg is compliant, as it already had compliant provisions before the directive.**

Managing directors, company managers (of entities established and/or VAT registered in Luxembourg), and both 'de jure' and 'de facto' managers responsible for daily operations may be held jointly and personally liable for breaches of VAT compliance obligations or the non-payment of VAT owed by the taxpayer under their management.

With regard to the penalties set out in **Article 9** of the PIF Directive, Luxembourg provides for:

- criminal fine: 500 EUR - 750,000 EUR and up to 6 times the evaded VAT in case of aggravated tax fraud;
- non-criminal fine: max €10,000 (Article 77 of the Luxembourg VAT law);
- temporary or permanent exclusion from public tenders.

Luxembourg has an **aggravating circumstance** for VAT fraud committed by organised criminal groups, according to Article 8 of the PIF Directive.

Malta

Malta **is now compliant with Article 3** of the PIF Directive. This compliance was achieved by **introducing a new legislation**, specifically Art. 2 of L. XVIII/2020 that amended Art. 190C⁹³ Maltese Criminal Code - Fraud affecting the Union's financial interests).

⁹³ **190C C.C.:**

(1) Whosoever intentionally commits fraud affecting the European Union's financial interests shall be liable, on conviction, to imprisonment for a term of six (6) months to four (4) years.

(2) For the purposes of this Sub-title, the following shall be regarded as fraud affecting the European Union's financial interests:

(a) in respect of non-procurement-related expenditure, any act or omission relating to:

(i) the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds or assets from the European Union budget or budgets managed by the European Union, or on its behalf.

(ii) non-disclosure of information in violation of a specific obligation, with the same effect; or

(iii) the misapplication of such funds or assets for purposes other than those for which they were originally granted.

(b) in respect of procurement-related.

expenditure, at least when committed in order to make an unlawful gain for the perpetrator or another by causing a loss to the European Union's financial interests, any act or omission relating to:

(i) the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the misappropriation or wrongful retention of funds or assets from the European Union budget or budgets managed by the European Union, or on its behalf.

(ii) non-disclosure of information in violation of a specific obligation, with the same effect; or

(iii) the misapplication of such funds or assets for purposes other than those for which they were originally granted, which damages the European Union's financial interests.

(c) in respect of revenue other than revenue arising from VAT own resources referred to in paragraph (d), any act or omission relating to:

(i) the use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the illegal diminution of the resources of the European Union budget or budgets managed by the European Union, or on its behalf.

(ii) non-disclosure of information in violation of a specific obligation, with the same effect; or

(iii) misapplication of a legally obtained benefit, with the same effect.

(d) in respect of revenue arising from VAT own resources, any act or omission committed in cross-border fraudulent schemes in relation to:

VAT fraud is classified as a **general offense (free-form)**, meaning no specific behaviors or actions are explicitly defined or required.

About the subjective element, Malta **applies liability for both intent and negligence**. Malta is, indeed, one of the seven MSs that foresees both elements, together with Cyprus, Denmark, Germany, Finland, Sweden and The Netherlands.

In relation to compliance with the penalties for committing fraud, described in Article 7 of the Directive, Malta complies, providing for a **maximum penalty of 4 years imprisonment** in cases where the fraud committed against the EU's financial interests had caused damage exceeding EUR 100,000 (the threshold for “considerable damage”).

With respect to compliance with Article 6 of the PIF Directive, concerning the liability of legal persons, **Malta is compliant thanks to the action of new legislations**.

Malta has an **aggravating circumstance** for the VAT fraud committed by organised criminal groups, according to Article 8 of the PIF Directive⁹⁴.

The Netherlands

In relation to compliance with Article 3 of the PIF Directive, **The Netherlands was already adequate and compliant**. Specifically, the relevant legal provisions are: Art. 225⁹⁵ (Document forgery), 227a⁹⁶ (False information to obtain benefits), 227b⁹⁷ (Failure to provide required information),

(i) the use or presentation of false, incorrect or incomplete VAT-related statements or documents, which has as an effect the diminution of the resources of the European Union budget.

(ii) non-disclosure of VAT-related information in violation of a specific obligation, with the same effect; or

(iii) the presentation of correct VAT-related statements for the purposes of fraudulently disguising the non-payment or wrongful creation of rights to VAT refunds.

⁹⁴ Article 190I:

The punishment for the offences referred to in articles 190C, 190D, 190E and 190F shall be increased by one to two degrees where the offence was committed within the framework of a criminal organisation within the meaning of Council Framework Decision 2008/ 841/JHA of 24 October 2008 on the fight against organised crime.

⁹⁵ Art. 225 CC:

“1 Anyone who falsely draws up or falsifies a document intended to serve as evidence of any fact, with the intention of using it as genuine and unadulterated or having it used by others, shall be guilty of forgery and punished with imprisonment of not more than six years or a fifth category fine.

2 Anyone who deliberately uses the forged or forged document as if it were genuine and unforged, or deliberately delivers or has such a document available, while he knows or should reasonably suspect that this document is intended for such use, shall be punished with the same penalty.

3 If an offense described in the first or second paragraph is committed with the intention of preparing or facilitating a terrorist crime, the prison sentence imposed for the offense will be increased by one third.”

⁹⁶ Art. 227a CC:

“Any person who, other than through forgery, deliberately does not provide truthful information to the person by whom or through whose intervention any benefit or compensation is provided, will, if the fact may serve to benefit himself or another, while he knows or must reasonably suspect that the information provided is important for determining his or another's right to such provision or compensation or for the amount or duration of such provision or compensation, punishable by a prison sentence of not more than four years or a fine of the fifth category.”

⁹⁷ Art. 227b CC:

“Any person who, in violation of an obligation imposed on him by or pursuant to a legal provision, deliberately fails to provide the required information in a timely manner will, if the fact may serve to benefit himself or another, while he knows or should reasonably suspect that the information are important for the determination of his or another's right to a benefit or compensation or for the amount or duration of such a benefit or compensation, punishable by a prison term of not more than four years or a fifth-category fine.”

323a⁹⁸ (Misuse of publicly provided resources), 420bis⁹⁹ (Money laundering), and 420ter¹⁰⁰ (Aggravated money laundering) of the Criminal Code, and Art. 68¹⁰¹ (Violation of tax obligations),

⁹⁸ Art. 323a CC:

“Any person who intentionally and unlawfully uses resources provided for a specific purpose by or on behalf of the government or by or on behalf of an international law organization for purposes other than those for which they were provided, shall be punished with a prison term of not more than four years or a fine of fifth category.”

⁹⁹ Art. 420bis CC:

“1 As guilty of money laundering, the penalty shall be a prison sentence of not more than six years or a fifth category fine for:

a. any person who conceals or conceals the true nature, origin, location, alienation or movement of an object, or conceals or conceals who is entitled to an object or who possesses it, while he knows that the object - directly or indirectly - originates from any crime.

b. anyone who acquires, possesses, transfers or converts an object or makes use of an object, while he knows that the object - directly or indirectly - originates from any crime.

2 Objects are understood to mean all property and all property rights.”

¹⁰⁰ Art. 420ter CC:

“Anyone who makes a habit of committing money laundering shall be punished with a prison term of not more than eight years or a fine of the fifth category.

2 Anyone who is guilty of money laundering in the exercise of his profession or business will be punished with the same penalty.”

¹⁰¹ Art. 68 Algemene wet inzake rijksbelastingen:

“1 The person who is obliged under the tax law to:

a. providing information, data or instructions, and not providing it, incorrectly or incompletely.

b. making books, documents, other data carriers or their contents available for consultation and not making them available for this purpose.

c. making books, documents, other data carriers or their contents available for consultation, and making them available for this purpose in a false or falsified form.

d. keeping records in accordance with the requirements set by or pursuant to the tax law, and not keeping such records.

e. keeping books, documents or other data carriers and not keeping them.

f. providing cooperation as referred to in Article 52, paragraph 6, and not providing it.

g. issuing an invoice or invoice, and providing an incorrect or incomplete invoice or invoice.

shall be punished with imprisonment for a term not exceeding six months or a fine of the third category.

2 Anyone who does not comply with the obligation imposed on him by Article 47, third paragraph, shall be punished with a fine of the second category.

3. It is not punishable for anyone who fails to comply with the obligation referred to in Article 47a as a result of a legal or judicial prohibition applicable to the body not established in the Netherlands or the natural person not residing in the Netherlands to cooperate in the provision of the requested data or information or making available for consultation books, documents, other data carriers or their contents, or as a result of a refusal by a body not established in the Netherlands or a natural person not residing in the Netherlands to provide the requested data or to provide information or to make books, documents, other data carriers or their contents available for consultation.

69¹⁰² (Tax evasion and fraudulent tax reporting) and 69a¹⁰³ (Tax evasion) and *Algemene wet Inzake Rijksbelastingen* (AWR - a Dutch law that establishes the general rules and procedures for the assessment and collection of national taxes, such as income tax, corporate tax, and value-added tax - VAT).

In the Netherlands, VAT fraud is classified as a **general offense (free-form)**, as for the majority of MSs.

About the subjective element, the Netherlands **applies liability for both intent and negligence**.

In relation to compliance with the sanctions for committing fraud, described in Article 7 of the Directive, the Netherlands complies, providing for a **maximum penalty of 4 years imprisonment** in cases where the fraud committed against the EU's financial interests had caused damage exceeding the threshold for "considerable damage". Depending on the conduct, this sanction can be up to 6 years.

With respect to compliance with Article 6 of the PIF Directive, concerning the liability of legal persons, **already had compliant provisions before the Directive** (Article 51 C.C.¹⁰⁴).

¹⁰² Art. 69 Algemene wet inzake rijksbelastingen:

"1 A person who deliberately fails to file a tax return provided for in the tax law, fails to file it within the prescribed period, or commits one of the facts described in Article 68, first paragraph, parts a, b, d, e, f or g, will be if the fact is that under-tax is levied, punished with a prison sentence of not more than four years or a fine of the fourth category or, if this amount is higher, not more than once the amount of the under-levy tax.

2 Anyone who deliberately submits a tax return provided for in the tax law incorrectly or incompletely, or commits the offense described in Article 68, first paragraph, part c, shall, if the fact results in too little tax being levied, be punished with a prison sentence of up to a maximum of six years or a fine of the fifth category or, if this amount is higher, a maximum of once the amount of the under-levied tax, on the understanding that insofar as the inaccuracy or incompleteness of the tax return relates to taxable income as referred to in Article 5.1 of the Income Tax Act 2001, the fine amounts to a maximum of three times the amount of the under-levied tax.

3 The right to prosecute on the basis of this article shall lapse if the guilty party still files a correct and complete report, or provides correct and complete information, data or indications before he knows or should reasonably suspect that one or more of the offenses referred to in Article 80, first paragraph, officials referred to, the inaccuracy or incompleteness is known or will become known. Notwithstanding the first sentence, the right to prosecute on the basis of this article does not lapse to the extent that the guilty party still files a correct and complete report, or provides correct and complete information, data or indications that relate to income from a substantial interest as referred to in Article 4.12 of the Income Tax Act 2001 or on income from savings and investments as referred to in Article 5.1 of that Act.

4 If the offense for which the suspect can be prosecuted falls under one of the provisions of the first or second paragraph, as well as under that of Article 225, second paragraph of the Criminal Code, criminal prosecution on the basis of the aforementioned Article 225, second paragraph, excluded.

5 Article 68, third paragraph, applies mutatis mutandis.

6 If the guilty person commits one of the criminal offenses described in the first and second paragraphs in his profession, he may be disqualified from practicing that profession."

¹⁰³ Art. 69a Algemene wet inzake rijksbelastingen:

"1 Anyone who deliberately fails to pay the tax that must be paid or remitted on the tax return, does not pay it in part, or does not pay it within the period set in the tax law, shall be punished with a prison sentence of not more than six years or a fine of the fifth category or, if this amount is higher, at most once the amount of the underpaid tax.

2 Article 69, sixth paragraph, applies mutatis mutandis.

3 It is not punishable for anyone who has requested the recipient in a timely manner to grant a deferral of payment or who has informed the recipient in writing immediately after it has become apparent that the body is unable to pay.

¹⁰⁴ Art. 51 CC:

"1 Criminal offenses can be committed by natural persons and legal entities.

About sanctions as indicated in **Article 9 of the PIF Directive**, The Netherlands foresees:

- criminal fine: extent may be up to 10% of the turnover in the previous year for sixth-category offenses if the maximum fine is inadequate.
- temporary or permanent disqualification from the practice of commercial activities.

The Netherlands has an **aggravating circumstance** for the VAT fraud committed by organised criminal groups, according to Article 8 of the PIF Directive.

Poland

In relation to compliance with **Article 3** of the PIF Directive, which concerns the criminalisation of the commission of fraud against the EU's financial interests, **Poland was already adequate**, specifically with Art. 270¹⁰⁵ (Forgery) and following¹⁰⁶ to Art. 277d of the Penal Code.

VAT fraud is classified as a **general offense (free-form)**, since Polish law – as in the majority of the other MSs - does not prescribe a specific method or means by which the crime must be committed. Instead, the focus is on the result or legal violation, regardless of how it was achieved.

About the subjective element, Poland provides that **only intentional acts** are punishable.

In relation to compliance with the sanctions for committing fraud, described in Article 7 of the Directive, Poland complies, providing for a **maximum penalty of 25 years imprisonment** in cases where the fraud committed against the EU's financial interests had caused damage exceeding EUR 100,000 (the threshold for “considerable damage”).

2 If a criminal offense is committed by a legal entity, criminal proceedings may be initiated and the penalties and measures provided for by law, if appropriate, may be imposed:

1°. against that legal entity, then

2°. against those who ordered the act, as well as against those who actually led the prohibited conduct, or

3°. against the persons mentioned under 1° and 2° together.

3 For the purposes of the previous paragraphs, the following are equated with the legal entity: the company without legal personality, the partnership, the shipping company and the target capital.

¹⁰⁵ Art. 270 C.C.:

Forgery

Chapter XXXIV. Offences against the Credibility of Documents.

§ 1. Anyone who forges, counterfeits or alters a document with the intention of using it as authentic, or who uses such a document as authentic, is liable to a fine, the restriction of liberty or imprisonment for between three months to five years.

§ 2. Anyone who fills in a form with someone else's signature, against the signatory's will and to his or her detriment, or who uses such a document, is liable to the same penalty.

§ 2a. If the act is of less significance, the offender is liable to a fine, the restriction of liberty or imprisonment for up to two years.

§ 3. Anyone who prepares for the offence specified in § 1 is liable to a fine, the restriction of liberty or imprisonment for up to two years.

¹⁰⁶ Art. 277a C.C.:

Forgery of invoices with an amount due exceeding PLN 10 million

Whoever commits the offence specified in Article 270a § 1 or Article 271a § 1 against an invoice or invoices containing a total amount of receivables the value or total value of which is greater than ten times the amount determining great value property,

shall be punishable by imprisonment for a term of between 5 and 25 years.

In the event of lesser gravity, the perpetrator of the act specified in § 1 shall shall be subject to the penalty of deprivation of liberty for up to 5 years.

Concerning compliance with Article 6 of the PIF Directive, related to the **liability of legal persons**, Poland already **had compliant provisions before the Directive**, specifically Art. 3 l. n. 659/2023 about the liability of legal persons and Article 116 of the Tax Ordinance¹⁰⁷.

About sanctions as indicated in **Article 9 of the PIF Directive**, Poland foresees non-criminal fines [see Art. 112b-112c of the Act of 11 March 2004 on the tax on goods and services].

Finally, also in Poland, there is the possibility to aggravate the penalty when the offender has acted in an **organised criminal group**.

Portugal

With respect to **compliance with Article 3 of the PIF Directive**, **Portugal is compliant**. This compliance is the result of a process: in December 2021, the European Commission initiated an infringement procedure against Portugal.

Portuguese legislation protects the EU's financial interests through two different legislations. The offense to VAT revenue through fraudulent action consisting in loss of VAT revenue is protected by Law 15/2021, which contains the offense of tax fraud (art. 103 e 104). Other non-tax revenues are protected by Decree-Law 28/84, through the crime of Fraud in obtaining a subsidy (art. 36),

¹⁰⁷ Article 116 of the Tax Ordinance

Tax liability of members of management boards of limited liability companies

The members of its management board shall be jointly and severally liable for the tax arrears of a limited liability company, a limited liability company in organisation, a simple joint-stock company, a simple joint-stock company in organisation, a joint-stock company or a joint-stock company in organisation with all their assets, if enforcement against the assets of the company has proved wholly or partly ineffective, and the member of the management board:

1) failed to prove that:

a) a bankruptcy petition was filed in due time or restructuring proceedings were opened at that time within the meaning of the Act of 15 May 2015. - Restructuring Law (Journal of Laws of 2022, item 2309 and of 2023, items 1723 and 1860) or an arrangement has been approved in the proceedings for the approval of an arrangement referred to in the Act of 15 May 2015. - Restructuring Law, or

b) the failure to file for bankruptcy was without his fault.

2) does not indicate the company's property from which enforcement will enable the company's tax arrears to be satisfied in a substantial part.

If the obligation to file a motion to declare bankruptcy arose and existed only at the time when enforcement by compulsory administration was conducted or by sale of the enterprise pursuant to the provisions of the Code of Civil Procedure, the failure to file a motion to declare bankruptcy shall be deemed to have occurred through no fault of the management board member referred to in § 1.

Liability of management board members includes tax arrears for obligations whose due date expired while they were acting as management board members, as well as arrears mentioned in Article 52 and Article 52a which arose while they were acting as management board members.

Persons performing the duties of a member of the management board at the time of the company's liquidation shall be liable for tax obligations arising under separate provisions after the company's liquidation, for tax arrears in respect of obligations whose due date expired after the company's liquidation, and for arrears listed in Article 52 and Article 52a arising after the company's liquidation. The provision of Article 115 § 4 shall apply accordingly.

Where a limited liability company in organisation, a simple joint-stock company in organisation or a joint-stock company in organisation does not have a management board, the company's proxy shall be liable for the company's tax arrears, or the partners shall be liable if the proxy has not been appointed. The provisions of § 1 and 2 shall apply mutatis mutandis.

The provisions of § 1-3 shall also apply to the former member of the management board and the former proxy or shareholder of the company in organisation.

In the case of a simple joint stock company in organisation in which a board of directors has been appointed, the provisions of § 1-4 shall apply mutatis mutandis to the board of directors and the directors.

Misappropriation of a subsidy (art. 37), and Misuse of EU revenues (art. 37-A¹⁰⁸). This latest addition, introduced in 2024 in that decree, sought to complete the transposition of the PIF Directive, especially regarding the use of benefits from European funds that did not fit into tax fraud (as they are not related to VAT) nor into fraud and diversion of obtaining subsidies (as they did not have an economic development purpose).

About the **objective element** of the crime, only some conducts are foreseen for revenues in general:

- the use or presentation of false, incorrect, or incomplete statements, or documents.
- misapplication of a legally obtained benefit.

and for VAT revenue, specifically:

- the use or presentation of false, incorrect or incomplete statements, or documents.
- non-disclosure of VAT-related information in violation of a specific obligation.
- the presentation of correct VAT-related statements to fraudulently disguise the non-payment or wrongful creation of rights to VAT refunds.

According to the Portuguese legislations, in order to qualify as a criminal offense, VAT fraud has to provide a tax advantage of 15,000 euros or more. Below this limit, it is an administrative offense.

With regard to the subjective element, Portugal provides that **only intentional acts are punishable**.

About compliance with the sanctions for committing fraud, described in **Article 7 of the Directive**, Portugal complies since their provision amounts to a **maximum of 8 years imprisonment** in cases where the fraud committed against the EU's financial interests had caused damage exceeding EUR 200,000 (even if for the EU, the threshold for “considerable damage” is 100,000).

With respect to compliance with **Article 6 of the PIF Directive**, concerning the liability of legal persons, Portugal was already compliant before the Directive, specifically with Article 3 of the DL 28/84 (Revenue other than VAT) and Art. 7 of the L 15/2001 (VAT Fraud) that foreseen criminal liability of the legal person.

About sanctions as indicated in Article 9 of the PIF Directive, Portugal foresees:

- exclusion from entitlement to public benefits or aid.
- temporary or permanent exclusion from public tender procedures.
- temporary or permanent disqualification from the practice of commercial activities.
- temporary or permanent closure of establishments that have been used for committing the criminal offense.

¹⁰⁸ Art. 37-A.C.C.:

Misuse of European Union revenue

1 - Anyone who uses a legally obtained benefit resulting from European Union revenue other than from value added tax own resources for a purpose other than that for which it was intended, and which involves a loss or advantage in an amount exceeding 100,000 (euro), shall be punished with imprisonment up to 5 years.

2 - When the facts set out in the previous paragraph involve a loss or advantage of an amount equal to or greater than 10,000 (euros) and less than or equal to 100,000 (euros), the perpetrator shall be punished with imprisonment up to 2 years or a fine up to 240 days.

3 - The same penalties shall apply to anyone who commits the conduct provided for in the preceding paragraphs by omission contrary to the duties of office.

As in the majority of MSs, also in Portugal when the offender has acted in an **organised criminal group**, the court may increase the sentence.

Romania

Romania achieved compliance with Article 3 of the PIF Directive by an amendment of the pre-existing discipline.

In December 2021, indeed, the European Commission initiated an infringement procedure for the delay in the transposition of the Directive.

The relevant legal references in this context are: Articles 9¹⁰⁹ and 9(1) Law 241/2005¹¹⁰ (Fraud); Art 18(3) Law 78/2000¹¹¹.

VAT fraud is classified as a **general offense (free-form)**, meaning no specific behaviors or actions are explicitly defined.

¹⁰⁹ Art. 9 Law 241/2005:

Constitutes tax evasion offences and is punishable by a penalty of two (2) to eight (8) years of imprisonment and the prohibition of certain rights or fines the following acts committed to evade the fulfillment of tax obligations:

- a) the concealment of the taxable or the taxable property or the source.
 - b) the omission, in whole or in part, of the evidence, in the accounting documents or other legal documents, of the commercial operations performed or of the realized revenues.
 - c) registration, in accounting documents or other legal documents, of the expenses that are not based on real operations or registration of other fictitious operations.
 - d) the alteration, destruction or concealment of accounting documents, memoranda of fiscal electronic cash registers or other means of storing data.
 - e) the execution of double accounts using documents or other means of storing data.
 - f) the avoidance of financial, tax or customs audits by non-disclosure, fictitious disclosure or inaccurate disclosure as to the principal or secondary premises of the verified persons.
 - g) the substitution, degradation or alienation by the debtor or by third parties of the seized goods in accordance with the provisions of the Tax procedure code and the Criminal procedure code.
- (2) If the facts referred to in paragraph (1) result in a prejudice of more than EUR 100 000, in the equivalent of the national currency, the minimum penalty limit provided by law is increased by 5 years.
- (3) If by the facts referred to in paragraph (1) result in a prejudice of more than EUR 500 000, in the equivalent of the national currency, the minimum penalty limit provided by law and its maximum limit is increased by 7 years.

¹¹⁰ Art. 9(1) Law 241/2005 as introduced by Law 125/2023:

(1) It is a criminal offence and is punishable by imprisonment from 7 to 15 years and the prohibition of the exercise of certain rights any action or inaction committed under fraudulent schemes of a cross-border nature having the effect reducing by at least 10,000,000 euros, in the equivalent of the national currency, the resources of the European Union budget, by:

- a) the use or presentation of false, incorrect or incomplete VAT-related statements or documents,
 - b) non-disclosure of VAT-related information in violation of a specific legal obligation,
 - c) the presentation of correct VAT-related statements for the purposes of fraudulently disguising the non-payment or wrongful creation of rights to VAT refunds.
- (2) The attempt to commit the criminal offense referred to in paragraph (1) shall be punished.

¹¹¹ Art 183 Law 78/2000:

(1) The use or presentation of false, incorrect or incomplete statements or documents, which has as its effect the illegal diminution of the resources of the Union budget or budgets managed by the Union, or on its behalf shall be punished with a penalty of two to seven years of imprisonment and prohibition of the exercise of certain rights.

(2) With the penalty provided in paragraph (1) shall be sanctioned the omission to provide, knowingly, the data required according to the legal provisions, whether the act results in the illegal diminution of the resources of the European Union budget or of the budgets administered or on its behalf.

With regard to the subjective element, Romania provides that **only intentional acts** are punishable. However, the national Expert clarified that **it is possible to punish an unintentional breach based on negligence if damage has been caused to European funds**, in conjunction with other provisions such as those on combating corruption and money laundering. Indeed, it is relevant that in Art. 185 Law 78/2000 for the prevention, discovery, and sanctioning of corruption deeds, with subsequent amendments and completions, also unintentional acts are punishable but only under certain conditions: *“Unintentional breach by the director, administrator or person responsible for deciding or controlling a legal person of a duty of service, by failing to perform it or by performing it improperly if the act resulted in the commission by a person who is subordinated to him and who acted on behalf of that legal person of one of the offenses referred to in art. 181-183 or committing a crime of corruption or money laundering in connection with the European Union funds, is punishable by a penalty of six months to three years imprisonment or a fine.”*

In relation to compliance with the sanctions for committing fraud described in Article 7 of the Directive, Romania complies since its provision amounts to a **maximum of 15 years imprisonment**, if the fraud committed against the EU's financial interests had caused damage exceeding EUR 100,000.

Art. 9 Law 241/2005 foresees three different penalties:

1. A “standard” penalty, for criminal offences with damages of less than EUR 100,000. This penalty is from two to eight years of imprisonment.
2. A first aggravating circumstance is if the damages are more than EUR 100,000 but less than EUR 500,000.

In this case, the penalty is from seven to thirteen years of imprisonment.

3. A second aggravating circumstance if the damages are more than EUR 500,000.

The penalty in this second option is from seven to thirteen years of imprisonment.

For the criminal offenses mentioned in Art. 91 Law 241/2005 there are more penalties, compliant with the PIF Directive (up to **15 years of imprisonment**).

About compliance with Article 6 of the PIF Directive, concerning the **liability of legal persons**, Romania already had compliant provisions before the PIF Directive [see Art. 135 Romanian criminal code¹¹²].

About sanctions as indicated in **Article 9 of the PIF Directive**, Romania foresees:

- criminal sanctions calculated based on the fine-days system, with specific rules depending on the severity of the offense and the legal entity's financial characteristics. Additionally, fines may be increased if the offense aimed to gain financial benefit.
- non-criminal fine (main penalty in the form of fines and ancillary penalties);
- temporary or permanent exclusion from public tender procedures.

¹¹² Art. 135 Conditions of criminal liability of the legal person

(1) The legal entity, except for the state and public authorities, is criminally liable for the offences committed in achieving the object of activity or in the interest or on behalf of the legal entity.

(2) Public institutions shall not be criminally liable for offences committed in the exercise of an activity that cannot be the subject of the private domain.

(3) The criminal liability of the legal entity does not exclude the criminal liability of the natural person who contributed to the commission of the same act.

- temporary or permanent disqualification from the practice of commercial activities.
- placing under judicial supervision.
- judicial winding-up.
- temporary or permanent closure of establishments that have been used for committing the criminal offense.

In Romania, if these behaviors are committed by organized criminal groups, an **aggravating circumstance** is foreseen.

Slovakia

Slovakia is still **not fully compliant with Article 3 of the PIF Directive**. While some amendments have been made to existing legislation, these changes still do not meet all the requirements outlined in the Directive.

In February 2022, indeed, the European Commission initiated an infringement procedure against Slovakia.

Slovakia is one of the 4 MSs that are not compliant, together with Croatia, Denmark, and France.

VAT fraud against EU is foreseen in Article 261 Slovakian Criminal Law¹¹³. It was first amended by L. 214/2019. Following amendments took place with Law 420/2019, 474/2019, 288/2020, 312/2020, 236/2021, Decision of the Constitutional Court of the SR 420/2023, 40/2024 (suspended effect), 47/2024.

¹¹³ § 261:

Damaging the Financial Interests of the European Union

(1) Anyone who uses or submits a falsified, incorrect, or incomplete report or document, or fails to provide required information, thereby enabling the unlawful retention of financial resources or other assets originating from the budget of the European Union, from a budget managed by the European Union, or on behalf of the European Union, or who uses such funds or assets for purposes other than those intended, shall be punished by imprisonment for a period of six months to three years.

(2) The same punishment as in paragraph 1 shall apply to anyone who uses financial resources or other assets originating from the budget of the European Union, from a budget managed by the European Union, or on behalf of the European Union for purposes other than those intended.

(3) A perpetrator shall be punished by imprisonment for a period of one to four years if, as an employee, member, representative, or any other person authorized to act on behalf of the entity providing financial resources or other assets mentioned in paragraph 1, they enable the acquisition of such resources or assets by someone they know does not meet the required conditions for their provision, or if they enable their unlawful retention or use for purposes other than those intended.

(4) A perpetrator shall be punished by imprisonment for a period of one to five years if they commit an act referred to in paragraph 1, 2, or 3

a) and cause significant damage,

b) out of a specific motive, or

c) in a more serious manner.

(5) A perpetrator shall be punished by imprisonment for a period of three to eight years if they commit an act referred to in paragraph 1, 2, or 3 and cause substantial damage.

(6) A perpetrator shall be punished by imprisonment for a period of seven to twelve years if they commit an act referred to in paragraph 1, 2, or 3:

a) and cause damage of a large scale, or

b) as a member of a dangerous organization.

VAT fraud is classified as a **general offense (free-form)**, meaning that no specific behaviors or actions are explicitly defined.

Concerning the subjective element, Slovakia provides that **only intentional acts** are punishable.

About sanctions described in Art. 7 of the Directive, Slovakia is not compliant and still inflicts a penalty of **less than 4 years in its maximum** in such cases. However, the penalty increases if the damage is significant (from 1 to 5 years) or substantial (from 3 to 8 years). At the same time, the penalty is increased to 7 to 12 years if the damage is on a large scale or if the crime is committed by a dangerous organization.

Regarding compliance with Article 6 of the PIF Directive, which addresses the **liability of legal persons**, Slovakia already had provisions in place that were compliant with the Directive, before its adoption [see Art. 4, Law n. 91/2016].

About sanctions indicated in Article 9 of the PIF Directive, Slovakia foresees:

- exclusion from entitlement to public benefits or aid;
- temporary or permanent exclusion from public tender procedures;
- temporary or permanent disqualification from the practice of commercial activities.

In Slovakia, if these behaviors are committed by organized criminal groups, an **aggravating circumstance** is foreseen, as already underlined.

Slovenia

Even though Slovenia did not respond to the questionnaire prepared for the EU Cyber VAT fraud project, it has nonetheless been possible to assess its **compliance** with the PIF Directive and **Article 3**. Specifically, the European Commission initiated an infringement procedure against Slovenia in February 2022 for its non-compliance with the Directive.

The relevant legal references are Article 254¹¹⁴ (Tax evasion) and Article 217¹¹⁵ C.C. (Fraud). It is also important to consider the Value Added Tax Act (ZDDV-1).

¹¹⁴ Article 254 C.C.:

Tax Evasion

(1) Whoever, with the intention either of evading, in whole or in part, the payment of income tax or any other prescribed tax or levy by himself or of enabling another person to do so, provides false information about income, expenses, property or other circumstances relevant to taxation, or otherwise defrauds the tax authorities, whereby the amount of tax evaded represents a major property benefit, shall be sentenced to imprisonment for not more than three years.

(2) Whoever, with the intention under the previous paragraph, fails to report income or other circumstances -whose report is mandatory, and which have an influence upon the assessment of tax obligations, whereby such obligations which he intended to evade represent a major property benefit, shall be punished to the same extent.

(3) If a major property benefit has been gained though the offence under the first or second paragraphs of the present article and the perpetrator intended to gain such property benefit, he shall be sentenced to imprisonment for not more than five years.

¹¹⁵ Article 217 C.C.:

(1) Whoever, with the intention of acquiring an unlawful property benefit for himself or a third person, by false representation or the suppression of facts leads another person into error or keeps him in error, thereby inducing him to perform an act or to omit to perform an act to the detriment of his or another's property shall be sentenced to imprisonment for not more than three years.

For the application of the criminal law on tax evasion, in Slovenia is required **intention**. Negligence is the subjective element of tax offences.

The foreseen sanctions are monetary (in daily amounts, depending on the weight of the offense) and **imprisonment from 1 to 8 years**. So, Slovenia complies with Article 7 of the PIF Directive.

In Slovenia it is possible to hold **legal entities responsible** for these crimes as well, so Slovenia is compliant also with Article 6 of the Directive.

In Slovenia, if these crimes are committed within the framework of **organized criminal groups**, the penalty is **more severe**.

(2) If a large loss of property has been incurred by the committing of the offence under the preceding paragraph, the perpetrator shall be sentenced to imprisonment for less than one and not more than eight years.

(3) If a minor loss of property has been incurred by the committing of the offence under the first paragraph of the present article and if the perpetrator's intention was to acquire a minor property benefit, he shall be punished by a fine or sentenced to imprisonment for not more than one year.

(4) Whoever, with the intention of causing damage to another person by false representation or the suppression of facts, leads a person into error or keeps him in error, thereby inducing him to perform an act or to omit to perform an act to the detriment of his or another's property shall be punished by a fine or sentenced to imprisonment for not more than one year.

(5) The prosecution for the offences under the third and fourth paragraphs of the present article shall be initiated upon a complaint.

Spain

With respect to **compliance with Article 3 of the PIF Directive, Spain is compliant** and achieved its compliance with the **amendment of pre-existing discipline**.

This process was completed after the deadline for the transposition of the Directive had expired, and in fact, in February 2022, the European Commission initiated an infringement procedure against Spain.

The relevant Spanish legislation on this matter is: Article 305¹¹⁶, 306¹¹⁷ of the Spanish Criminal Code (contains the criminal conduct related to VAT in Art. 3 of the PIF Directive), 305 bis¹¹⁸

¹¹⁶ Article 305 of the Spanish Criminal Code:

1. Anyone who, by action or omission, defrauds the state, regional, foral or local Public Treasury, evading the payment of taxes, amounts withheld or which should have been withheld or payments on account, unduly obtaining refunds or enjoying tax benefits in the same way, provided that the amount of the defrauded amount, the unpaid amount of the withholdings or payments on account or of the refunds or tax benefits unduly obtained or enjoyed exceeds one hundred and twenty thousand euros, shall be punished with a prison sentence of one to five years and a fine of one to six times the aforementioned amount, unless they have regularised their tax situation under the terms of paragraph 4 of this Article.

The mere submission of declarations or self-assessments does not exclude fraud, where it is established by other facts.

In addition to the aforementioned penalties, the person responsible shall lose the possibility of obtaining public subsidies or aid and the right to enjoy tax or Social Security benefits or incentives for a period of three to six years.

2. For the purposes of determining the amount mentioned in the previous section:

a) In the case of taxes, withholdings, payments on account or refunds, periodic or periodically declared, the amount defrauded in each tax period or declaration period shall be taken as the amount defrauded, and if these are less than twelve months, the amount defrauded shall refer to the calendar year. Notwithstanding the above, in cases where the fraud is carried out within a criminal organisation or group, or by persons or entities acting under the guise of a real economic activity without actually carrying it out, the offence shall be prosecutable from the moment the amount set out in paragraph 1 is reached.

b) In all other cases, the amount shall be understood to refer to each of the different concepts for which a taxable event is liable for assessment.

3. The same penalties shall be imposed on anyone who commits the conduct described in paragraph 1 and on anyone who evades the payment of any amount due or takes undue advantage of a legally obtained benefit, when the acts are committed against the Treasury of the European Union, provided that the amount defrauded exceeds one hundred thousand euros within a period of one calendar year. Notwithstanding the foregoing, in cases where the fraud is carried out within a criminal organisation or group, or by persons or entities acting under the guise of a real economic activity without actually carrying it out, the offence shall be prosecutable from the moment the amount set out in this section is reached.

If the amount defrauded does not exceed one hundred thousand euros but exceeds ten thousand euros, a prison sentence of three months to one year or a fine of three times the aforementioned amount and the loss of the possibility of obtaining public subsidies or aid and the right to enjoy tax or Social Security benefits or incentives for a period of six months to two years shall be imposed.

4. The tax situation shall be deemed to be regularised when the taxpayer has fully acknowledged and paid the tax debt before the Tax Administration has been notified of the commencement of verification or investigation proceedings aimed at determining the tax debts that are the subject of the regularisation or, in the event that such proceedings have not taken place, before the Public Prosecutor's Office, the State Attorney or the procedural representative of the regional, provincial or local administration in question files a complaint or accusation against him or her, or before the Public Prosecutor's Office or the Examining Magistrate carries out actions that allow him or her to have formal knowledge of the initiation of proceedings. Likewise, the effects of the regularisation provided for in the previous paragraph shall be applicable when tax debts are paid once the Administration's right to determine them in administrative proceedings has lapsed.

The regularisation by the taxpayer of his tax situation shall prevent him from being prosecuted for possible accounting irregularities or other instrumental falsehoods which, exclusively in relation to the tax debt subject to regularisation, he may have committed prior to the regularisation of his tax situation.

5. When the Tax Administration sees indications that an offence against the Public Treasury has been committed, it may settle separately, on the one hand, those items and amounts that are not linked to the possible offence against the Public Treasury, and on the other, those that are linked to the possible offence against the Public Treasury.

The settlement indicated in the first place in the previous paragraph will follow the ordinary procedure and will be subject to the system of appeals inherent to all tax settlements. And the settlement that may arise from those concepts and amounts that are linked to the possible offence against the Public Treasury shall follow the procedure established for this purpose in the tax regulations, without prejudice to the final adjustment to what is decided in the criminal proceedings.

The existence of criminal proceedings for an offence against the Treasury will not paralyse the action to collect the tax debt. The Tax Administration may initiate collection proceedings, unless the Judge, either ex

(Aggravating circumstances); Ley Orgánica 1/2019 amends section 3 of art. 305 of the Spanish Criminal Code. Art. 306 of the Spanish Criminal Code is amended by Ley Orgánica 9/2021.

VAT fraud is classified as a **general offense (free-form)**, meaning that no specific behaviors or actions are explicitly defined. All possible conducts of VAT fraud are covered.

The Spanish Criminal Code does not provide for specific forms of tax fraud, it only provides for tax fraud, which may consist of evading payments, enjoying undue benefits, or using the funds obtained for purposes other than lawful. However, the specific form is not provided (use of false or incorrect documents; omission of information; declaration of incorrect data, etc.).

About the subjective element, Spain provides that **only intentional acts** are punishable.

officio or at the request of a party, has ordered the suspension of the enforcement proceedings, subject to the provision of a guarantee. If it is not possible to provide a guarantee in whole or in part, the Judge may exceptionally order the suspension with total or partial waiver of guarantees if he considers that the enforcement could cause irreparable damage or damage that would be very difficult to repair.

6. The Judges and Courts may impose on the taxpayer or the perpetrator of the offence the penalty that is one or two degrees lower, provided that, within two months of the judicial summons as a defendant, he/she pays the tax debt and judicially acknowledges the facts. The above shall also apply to participants in the offence other than the taxpayer or the perpetrator of the offence, when they actively collaborate in obtaining decisive evidence for the identification or capture of other perpetrators, for the complete clarification of the criminal acts or for the ascertainment of the assets of the taxpayer or of other perpetrators of the offence.

7. In proceedings for the offence referred to in this Article, for the enforcement of the fine and civil liability, which shall include the amount of the tax debt that the Tax Administration has not settled due to the statute of limitations or any other legal cause under the terms provided for in Law 58/2003, General Taxation Act, of 17 December, including interest on late payment, the Judges and Courts shall seek the assistance of the Tax Administration services, which shall demand them through the administrative procedure of enforcement under the terms established in the aforementioned Act.

¹¹⁷ Art. 306 of the Spanish Criminal Code:

Any person who by act or omission defrauds the general budgets of the European Union or other budgets administered by it of more than fifty thousand euros, by evading, except in the cases referred to in Article 305(3), the payment of sums due or, except in the cases referred to in Article 308, by putting the funds obtained to a use other than that for which they were intended or by improperly obtaining funds by falsifying the conditions required for their grant or concealing the fact that they would have prevented their being granted, shall be punished by imprisonment for a term of one year, the funds obtained for a use other than that for which they were intended or unduly obtaining funds by falsifying the conditions required for their concession or concealing those that would have prevented it, shall be punished with a prison sentence of one to five years and a fine of one to six times the aforementioned amount and the loss of the possibility of obtaining public subsidies or aid and the right to enjoy tax or Social Security benefits or incentives for a period of three to six years.

If the amount defrauded or misapplied does not exceed fifty thousand euros, but exceeds four thousand euros, a prison sentence of three months to one year or a fine of three times that amount and the loss of the possibility of obtaining public subsidies or aid and the right to enjoy tax or Social Security benefits or incentives for a period of six months to two years shall be imposed.

¹¹⁸ Art. 305 bis of the Spanish Criminal Code:

1. The offence against the Public Treasury shall be punishable with a prison sentence of two to six years and a fine of twice to six times the amount defrauded when the fraud is committed in any of the following circumstances:

- a) The amount of the amount of the defrauded quota exceeds six hundred thousand euros.
- b) That the fraud has been committed within an organisation or criminal group.
- c) That the use of natural or legal persons or interposed unincorporated entities, businesses or fiduciary instruments or tax havens or territories of non-taxation hides or hinders the determination of the identity of the taxpayer or of the person responsible for the offence, the determination of the amount defrauded or of the assets of the taxpayer or of the person responsible for the offence.

2. All the other provisions contained in Article 305 shall apply to the cases described in this Article.

In these cases, in addition to the penalties indicated, the person responsible shall be subject to the loss of the possibility of obtaining public subsidies or aid and the right to enjoy tax or Social Security benefits or incentives for a period of four to eight years.

In relation to compliance with the penalties for committing fraud, described in Article 7 of the Directive, Spain complies, providing for a **maximum penalty of 5 years imprisonment** in cases where the fraud committed against the EU's financial interests had caused damage exceeding EUR 100,000 (the threshold for “considerable damage”).

To comply with **Article 6 of the PIF Directive**, Spain **amended its pre-existing legislation despite it already being adequate** [see Article 310 bis C.C.¹¹⁹ - specific provision for criminal liability of legal persons for tax fraud offenses and Article 31 bis¹²⁰ - general provision for criminal liability of legal persons].

¹¹⁹ Art. 310 bis Spanish Criminal Code:

When, in accordance with the provisions of Article 31 bis, a legal person is responsible for the offences set out in this Title, the following penalties shall be imposed on that person:

- a) a fine of as much as twice the amount defrauded or wrongfully obtained, if the offence committed by the natural person is punishable by a term of imprisonment of more than two years.
- b) a fine of two to four times the amount defrauded or wrongfully obtained, if the offence committed by the natural person is punishable by a term of imprisonment of more than five years
- c) A fine of six months to one year, in the cases referred to in Article 310.

In addition to the aforementioned, the legal person responsible shall be subject to the loss of the possibility of obtaining public subsidies or aid and the right to enjoy tax or Social Security benefits or incentives for a period of three to six years. The prohibition to contract with the Public Administrations may be imposed.

In accordance with the rules laid down in Article 66 bis, the judges and courts may also impose the penalties set out in Article 33(7)(b), (c), (d), (e) and (g).

¹²⁰ Art. 31 bis Spanish Criminal Code:

1. In the cases provided for in this Code, legal persons shall be criminally liable:

a) For offences committed in the name of or on behalf of them, and for their direct or indirect benefit, by their legal representatives or by those who, acting individually or as members of an organ of the legal person, are authorised to take decisions on behalf of the legal person or hold powers of organisation and control within the legal person.

b) Offences committed, in the exercise of corporate activities and on behalf of and for the direct or indirect benefit of the same, by those who, being subject to the authority of the natural persons mentioned in the previous paragraph, have been able to carry out the acts because they have seriously failed to comply with their duties of supervision, monitoring and control of their activity in view of the specific circumstances of the case.

2. If the offence is committed by the persons referred to in point (a) of the preceding paragraph, the legal person shall be exempt from liability if the following conditions are met:

1°. the management body has adopted and effectively implemented, prior to the commission of the offence, organisational and management models that include the surveillance and control measures suitable for preventing offences of the same nature or for significantly reducing the risk of their commission.

2°. the supervision of the operation of and compliance with the prevention model in place has been entrusted to an organ of the legal person with autonomous powers of initiative and control or which is legally entrusted with the function of supervising the effectiveness of the legal person's internal controls.

3°. the individual perpetrators have committed the offence by fraudulently circumventing the organisational and preventive models, and

4°. there has been no omission or insufficient exercise by the body referred to in condition 2 of its supervisory, monitoring and control functions.

In cases in which the above circumstances can only be partially accredited, this circumstance shall be assessed for the purposes of mitigating the sentence.

3. In the case of small legal persons, the supervisory functions referred to in Condition 2.2 may be assumed directly by the management body. For these purposes, small legal persons are those which, according to the applicable legislation, are authorised to submit abridged profit and loss accounts.

4. If the offence was committed by the persons referred to in paragraph 1(b), the legal person shall be exempted from liability if, prior to the commission of the offence, it has adopted and effectively implemented an organisational and management model which is suitable to prevent offences of the nature of the offence committed or to reduce significantly the risk of its commission.

In this case, the mitigation provided for in the second subparagraph of paragraph 2 of this Article shall also apply.

About sanctions indicated in **Article 9** of the PIF Directive, Spain foresees:

- criminal fine (main penalty);
 - a fine of up to twice the amount defrauded or wrongfully obtained if the offense is punishable by more than two years in prison (applied in basic cases);
 - a fine of two to four times the amount defrauded or wrongly obtained if the offense is punishable by more than five years in prison (applied in aggravated cases of Article 305 bis.1 of the Spanish Criminal Code).

Aggravating factors include:

- the defrauded amount exceeds 600,000 euros;
 - the fraud was committed within an **organization or criminal groups**;
 - the use of natural or legal persons, unincorporated entities, businesses, fiduciary instruments, tax havens, or no-taxation territories to hide or obstruct the determination of the identity of the taxpayer, the amount defrauded, or the assets involved;
- exclusion from entitlement to public benefits or aid (main penalty);
 - temporary or permanent exclusion from public tender procedures (main penalty);
 - temporary or permanent disqualification from the practice of commercial activities (additional penalty);
 - placing under judicial supervision (additional penalty);
 - judicial winding-up (additional penalty);
 - temporary or permanent closure of establishments that have been used for committing the criminal offense (additional penalty).

In Spain, if these behaviors are committed by organized criminal groups, an **aggravating circumstance** is foreseen.

Sweden

Regarding compliance with **Article 3** of the PIF Directive, Sweden **meets the requirements** through an **amendment to pre-existing legislation**. The European Commission initiated an infringement

5. The organisation and management models referred to in condition 1 of section 2 and the previous section shall meet the following requirements:

1°. They shall identify the activities in the scope of which the offences to be prevented may be committed.

2°. They shall establish protocols or procedures that specify the process for the formation of the legal person's will, the adoption of decisions and their execution in relation to them.

3°. They shall have appropriate financial resource management models to prevent the commission of crimes that must be prevented.

4°. They shall impose the obligation to report possible risks and breaches to the body responsible for overseeing the operation and compliance of the prevention model.

5°. Establish a disciplinary system that adequately sanctions non-compliance with the measures established in the model.

6° Periodic verification of the model and its possible modification when relevant breaches of its provisions are revealed, or when changes occur in the organisation, control structure or activity carried out that make them necessary.

procedure against Sweden in February 2022. Additionally, the Supreme Court case B5072-17 confirmed compliance.

VAT fraud in Sweden is classified as a general offense (**free-form**), meaning that no specific behaviors or actions are explicitly defined.

With regard to the subjective element, Sweden applies liability for **both intent and negligence**.

Regarding compliance with the penalties for fraud outlined in **Article 7** of the Directive, Spain meets the requirements by imposing a maximum sentence of **six years imprisonment** for cases where fraud against the EU's financial interests results in damage exceeding EUR 100,000, the threshold for "considerable damage" [see Section 4 of The tax crime act 1971:69¹²¹].

Sweden had compliant provisions in place before the PIF Directive regarding compliance with Article 6, which addresses the **liability of legal persons** [see Section 37, art. 7, Swedish criminal code].

In relation to the sanctions listed in **Article 9** of the PIF Directive, Sweden only provides a criminal fine (not specified).

In Sweden, if these behaviors are committed by organized criminal groups, an **aggravating circumstance** is foreseen.

3.2 General considerations and concluding remarks

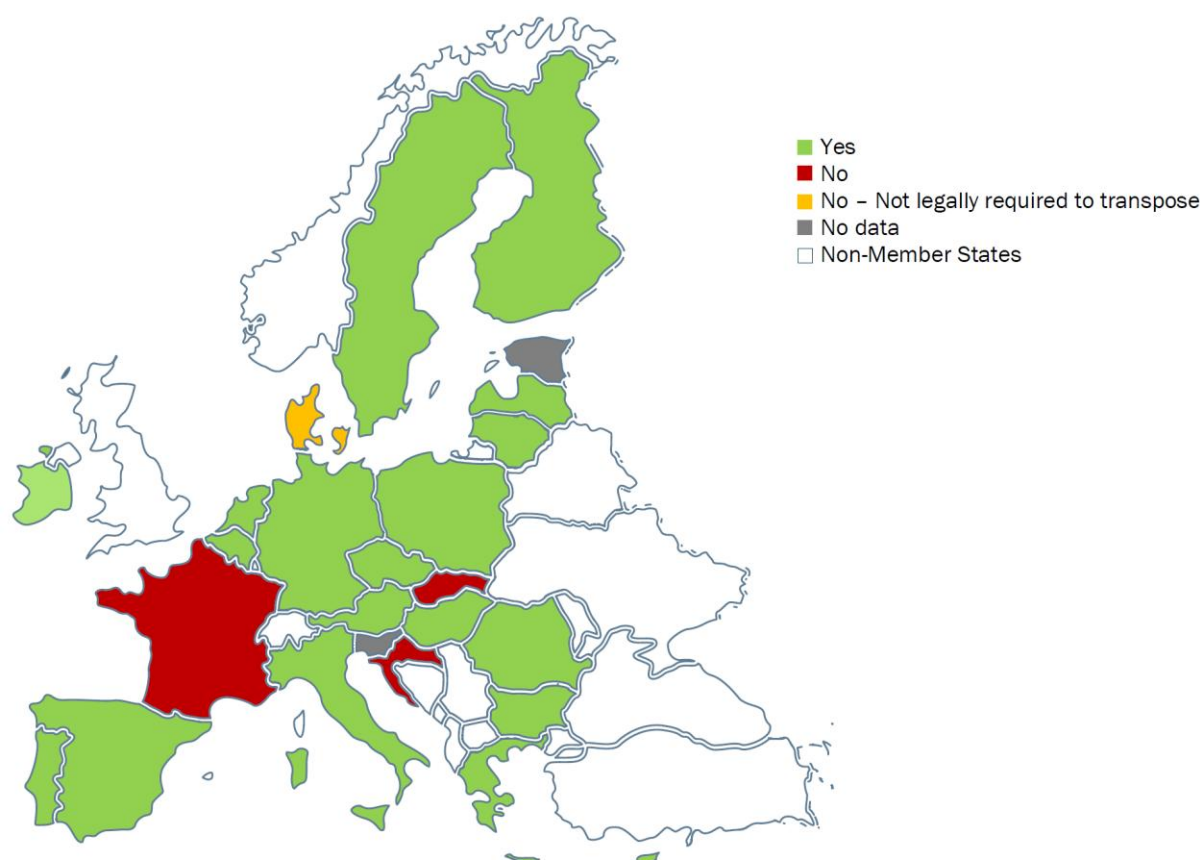
Compliance with Article 3 of the PIF Directive

From the analysis of the regulations and the answers of the national experts of each Member State, it can be concluded that most of the MSs are compliant with Article 3 of the PIF Directive (21 out of the 25 respondents). Four of them (**Croatia, Denmark, France, and Slovakia**), instead, did not transpose the Directive: among them, Denmark was not legally required to transpose it, the other two (**Croatia and Slovakia**) had implemented some amendments to their previous legislation, still not meeting the requirements, and only one (**France**) did not amend the legislation at all (even if it seems to be compliant because there is no infringement procedure of the European Commission against France).

¹²¹ Section 4 of the Tax Crime act 1971:69

If the crime referred to in section 2 is considered serious, the person is sentenced for serious tax fraud to imprisonment, for no less than six months and no more than six years.

Fig. 1: Answer to question 1: “Does your country’s national legislation on VAT fraud committed by natural persons comply with Article 3 of the PIF Directive?” EU Member States. N=25. Year 2024.

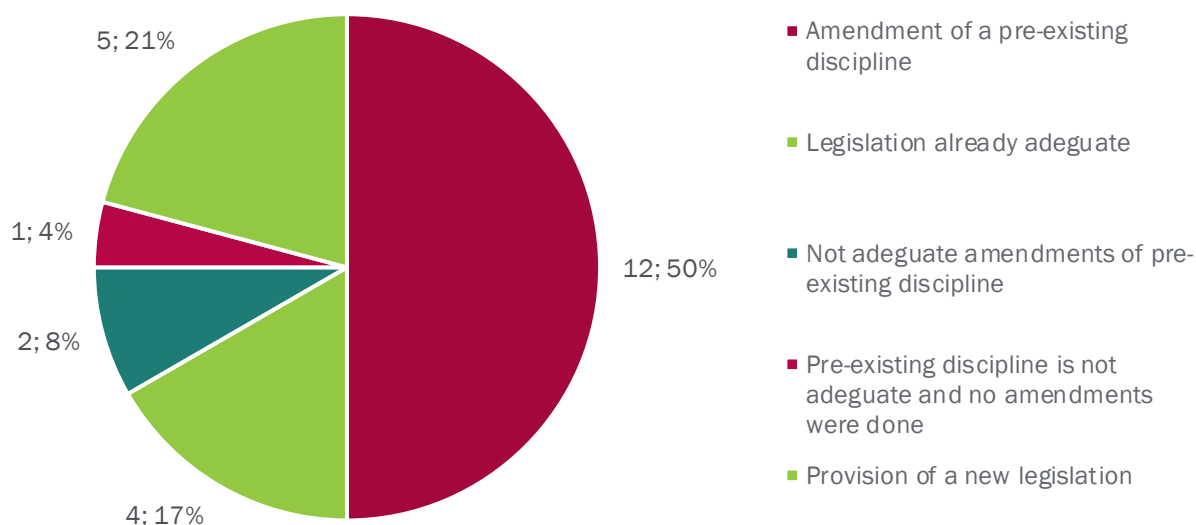


Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

In addition to examining the compliance of the MSs, it was also investigated how compliance was achieved (Fig. 2): 12 MSs amended their pre-existing legislation (**Belgium; Bulgaria; Czech Republic; Germany; Ireland; Lithuania; Luxembourg; Portugal; Romania; Spain; Sweden**), 5 MSs (**Austria; Cyprus; Greece; Latvia; Malta**) introduced entirely new legislation, and 3 (**Hungary; Poland; The Netherlands**) already had provisions that were compliant with the Directive.

Conversely, a Member State (**France**) did not take any action to become compliant, and another (**Denmark**) was not legally required to do so. Finally, in two cases (**Croatia** and **Slovakia**), despite the adoption of amendments, they were not sufficient.

Fig. 2: Article 3 of the PIF Directive and national provisions. Absolute number and percentage value of EU Member States. N=24. Year 2024.



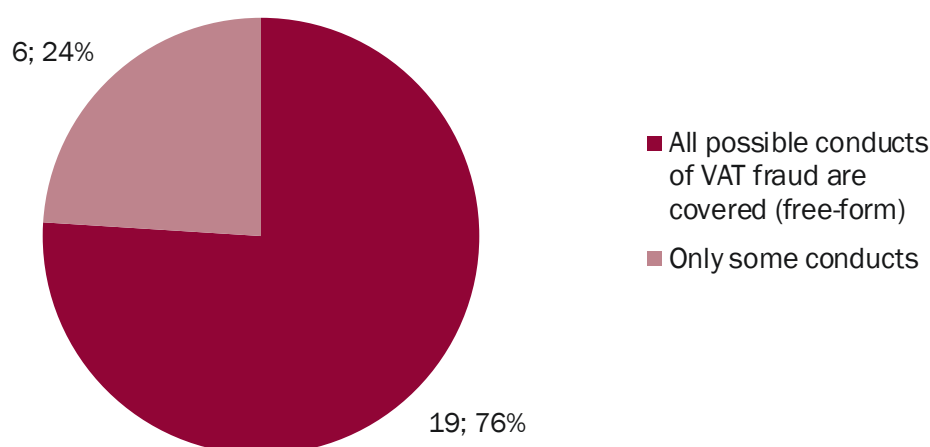
Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

Although **Finland** is compliant with Article 3 of the PIF Directive, as stated in Government Proposal No. 231/2018; according to Finland's national expert, no significant changes were necessary to achieve compliance, indicating that the existing frameworks and legislation were already in line with the requirements of the Directive.

Objective element of the VAT-related offenses

In most MSs (19 out of 25), VAT fraud is classified as a general offense (free-form), meaning no specific behaviors or actions are explicitly defined (Fig. 3). Only 6 MSs (**Bulgaria, Croatia, France, Greece, Portugal, and Italy**) prescribe specific, binding actions in their criminal codes (Fig. 4).

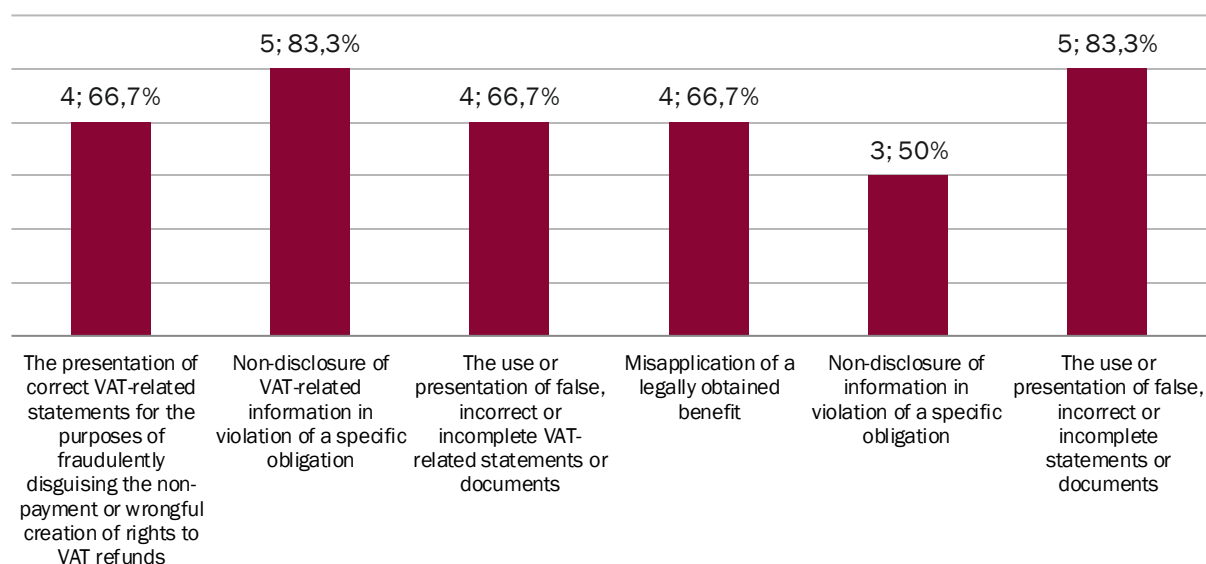
Fig. 3: Answer to question 1.1(a): “Which of the following acts fall under your national offence(s) of VAT fraud by national persons?”. Absolute number and percentage value of EU Member States. N=25. Year 2024.



Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

Article 3 of the Directive outlines certain actions that constitute VAT fraud against the EU. Among these, the MSs that do not classify VAT fraud as a general offense specify particular actions. In some cases, additional actions are included beyond those indicated in Article 3, while in others, not all of the specified actions are explicitly covered.

Fig. 4: Answer to question 1.1(b): “If only some conducts, which ones?”. Absolute number and percentage value of EU Member States. N=6. Year 2024.



Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

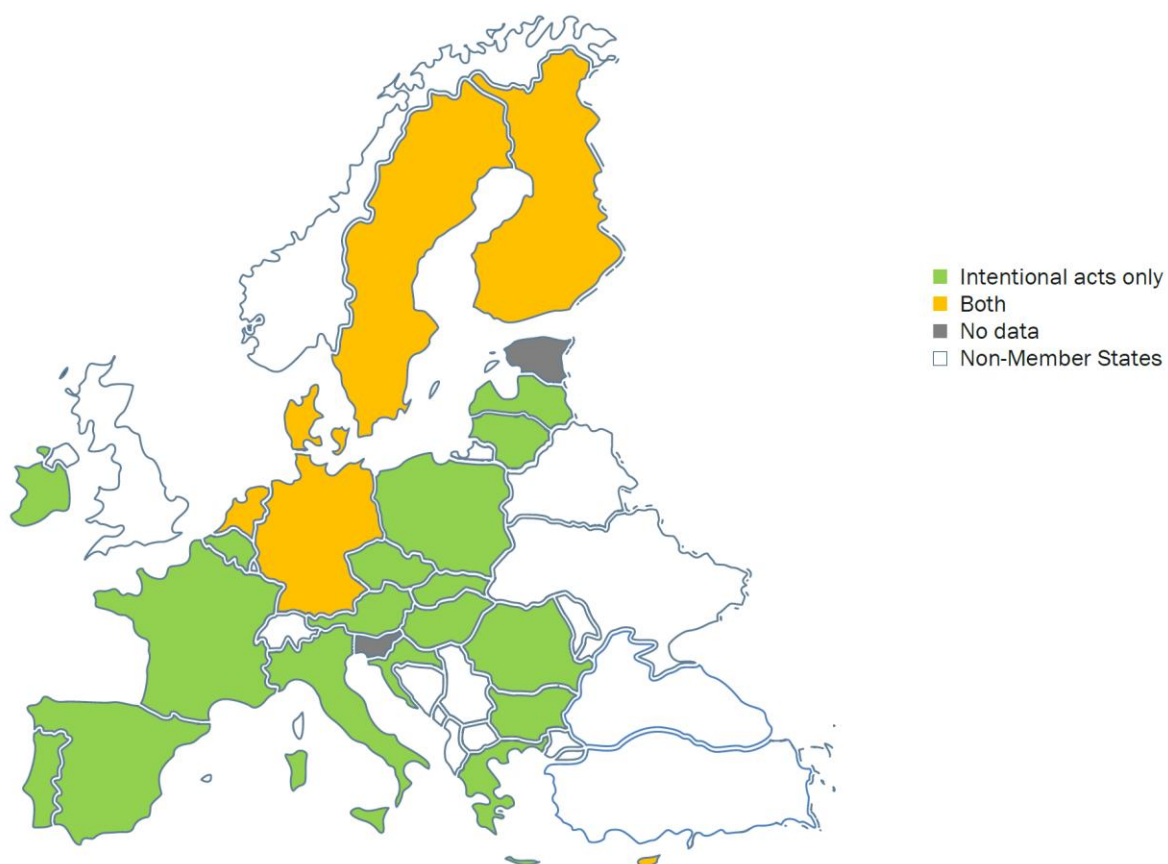
Subjective element of the VAT-related offenses

Almost two-thirds of the responding MSs (18 out of 25) only foresee criminal liability for VAT fraud when committed with intent.

None of the MSs apply criminal liability exclusively for negligence (*culpa*), while seven states apply liability for both intent and negligence (**Cyprus, Denmark, Finland, Germany, Malta, The Netherlands, and Sweden** – Fig. 5).

As already specified in the dedicated section, although **Romania** initially replied that VAT fraud is only punishable if committed intentionally, it later clarified that it is possible to punish an unintentional breach on the basis of negligence if damage has been caused to European funds, in conjunction with other provisions such as those on combating corruption and money laundry.

Fig. 5: Answer to question 1.2: “Which acts (1.1) are punishable with regard to the subjective elements of your national criminal offence of VAT fraud?”. EU Member States. N=25. Year 2024.

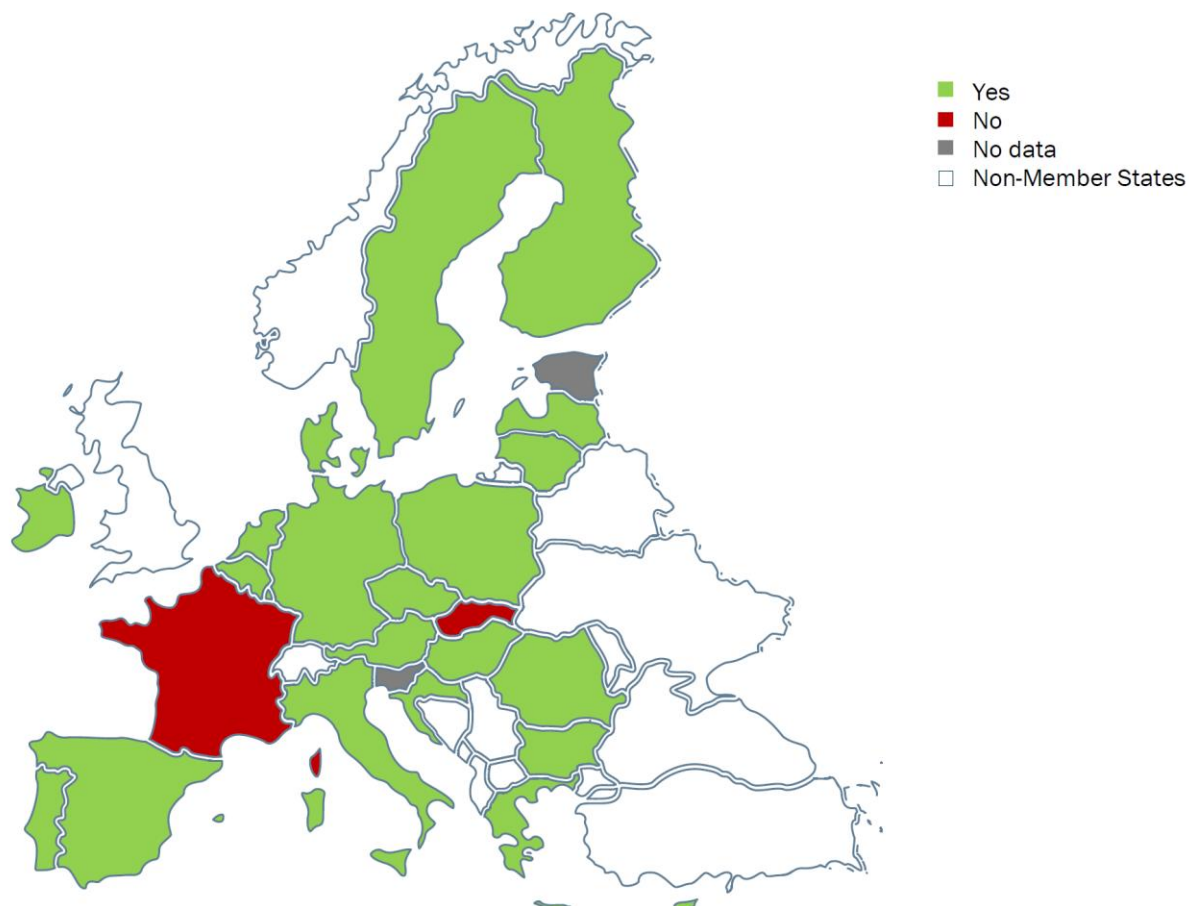


Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

Compliance with Article 7 of the PIF Directive

Annex 2 delved into **compliance with the required sanctions for the commission of fraud, described in Art. 7 of the Directive** (Fig. 6). Specifically, the question concerned compliance with the required maximum sentence of at least 4 years of imprisonment in cases where the fraud committed against the financial interests of the EU had led to damage of over 100.000 € (threshold established for the “considerable damage”).

Fig. 6: Answer to question 2: “Is your national law in line with Article 7 of the PIF Directive with regard to sanctions for natural persons committing VAT fraud?”. EU Member States. N=25. Year 2024.

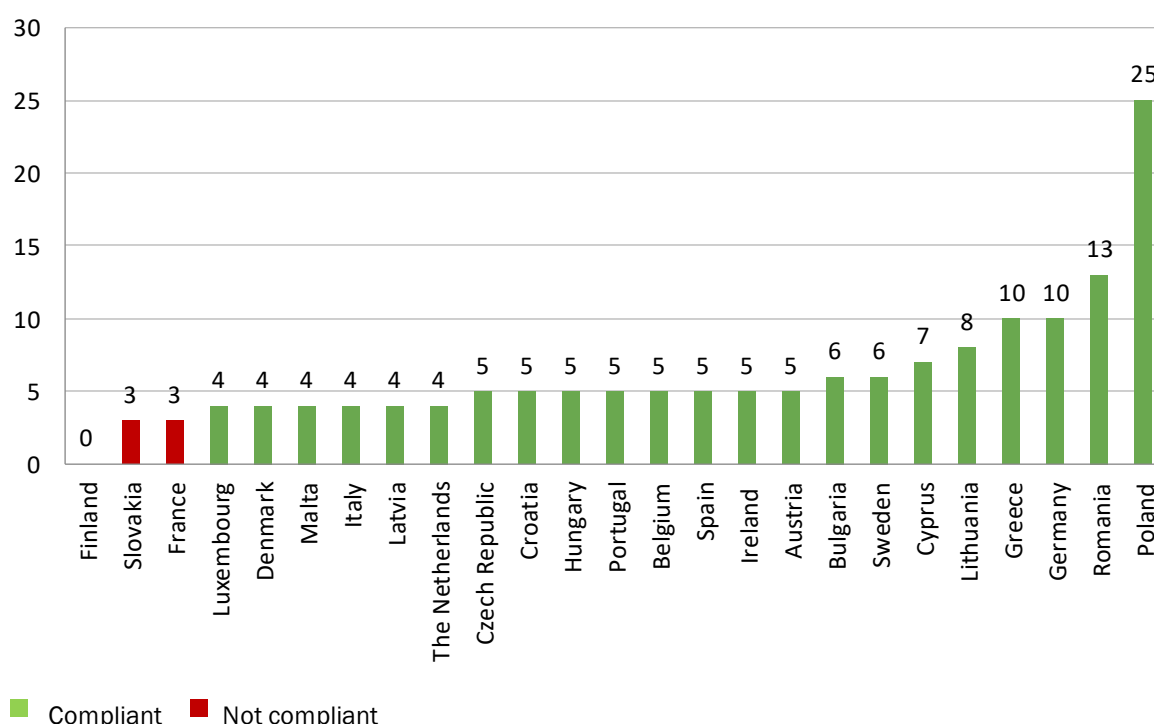


Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

The findings indicate that only two states (**France and Slovakia**) still impose a penalty of less than four years in its maximum in such cases. France provides various penalties depending on the different offenses that may encompass VAT fraud, as there is no specific article dedicated to this crime. Regarding **Greece**, the national legislation does not stipulate a maximum sentence, but rather a minimum sentence of 10 years (Fig. 7).

In **Finland** emerged a particular case: although their provision amounts to a maximum of two years imprisonment and thus could not be compliant, compliance with Article 7 of the PIF Directive seems to be achieved by the joint provision of other articles of the Finnish Criminal Code (RL), in particular fiscal crimes and crimes against the Public Administration.

Fig. 7: Answer to question 2: “Is your national law in line with Article 7 of the PIF Directive with regard to sanctions for natural persons committing VAT fraud?”. Maximum years of imprisonment in EU Member States when the fraud has led to damage of over 100.000€ (absolute number). Compliance of EU Member States with the required maximum penalty of at least four years of imprisonment. N=25. Year 2024.



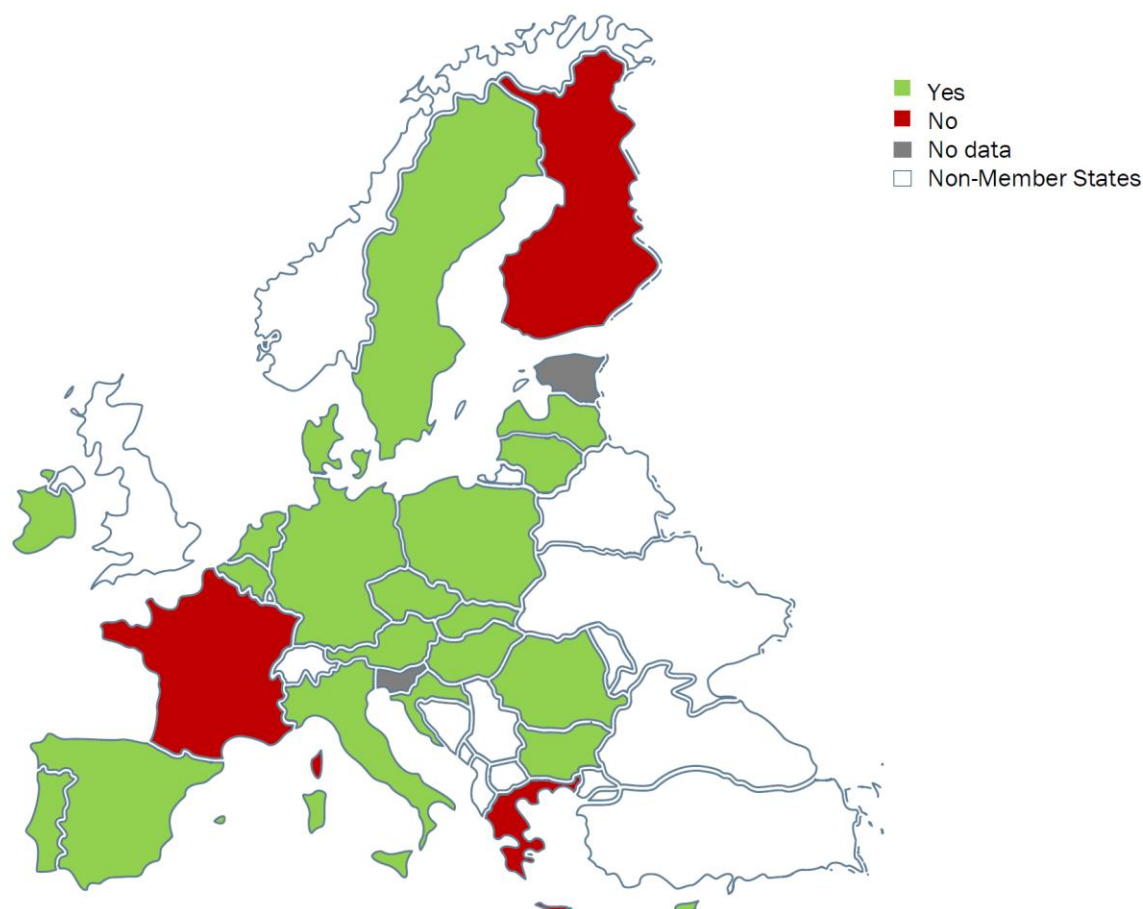
Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

Aggravating circumstances for VAT fraud committed within a criminal organisation

Only one-fifth of the responding MSs (3 up to 25) do not provide for an **aggravating circumstance** in cases of VAT fraud committed by an organized criminal group, as stipulated in Article 8 of the PIF Directive.

Beyond the numerical data from the questionnaires, it is clear that all countries provide an aggravating factor for crimes committed within the context of organized crime. Those without specific provisions for VAT fraud apply common aggravating factors that can be applied to all offenses (e.g. France and Greece). Finland, on the other hand, directly refers to Framework Decision 2008/841/JHA.

Fig. 8: Answer to question 3: “Does your national law contain an aggravating circumstance for the commission of VAT fraud in the context of organized crime, as provided for in Article 8 of the PIF Directive?”. EU Member States. N=25. Year 2024.

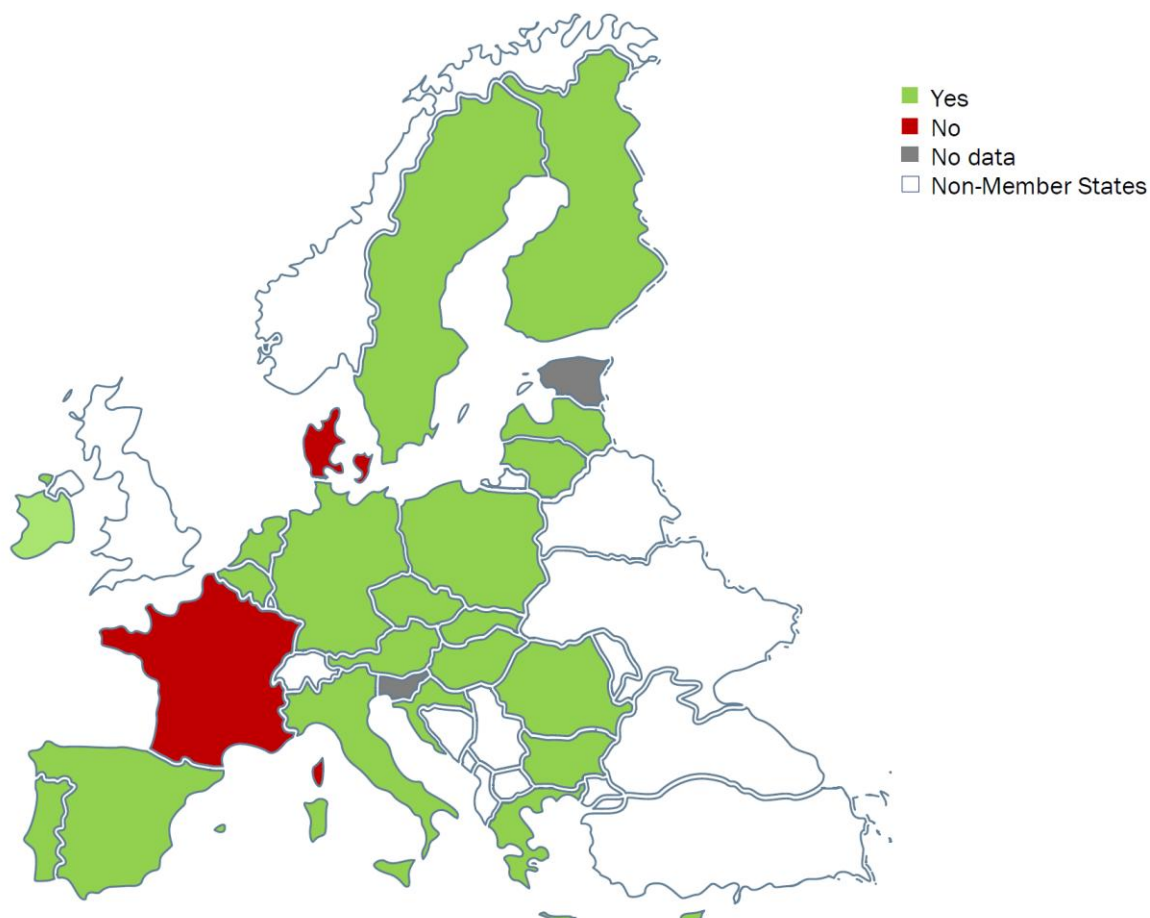


Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

Compliance with Article 6 of the PIF Directive

Lastly, Annex 3 was dedicated to the assessment of the **compliance with Art. 6 of the PIF Directive**, involving the liability of legal persons: 23 States out of 25, whether through amendments, new disciplines, or because they were already compliant, correctly transposed the PIF Directive regarding these aspects. Two of them (**Denmark and France**) did not: **Denmark** because it is not legally required to transpose it, being however bound by the PIF Convention; **France** has not yet amended its legislation. However, even in France, corporate liability for crimes is foreseen.

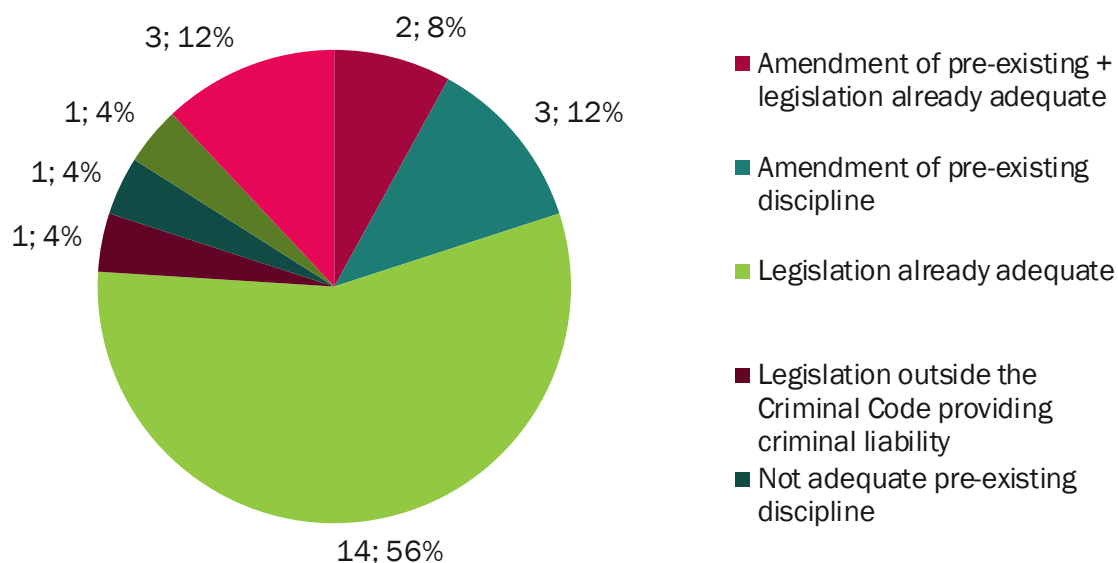
Fig. 9: Answer to question 4: “Is your national law on VAT fraud in relation to the liability of legal persons compliant with Article 6 of the PIF Directive?”. EU Member States. N=25. Year 2024.



Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

As for the way of achievement (Fig. 10) of compliance with Article 6, 14 MSs (**Austria; Belgium; Croatia; Czech Republic; Germany; Hungary; Latvia; Lithuania; Luxembourg; Poland; Romania; Slovakia; Sweden; The Netherlands**) already had compliant provisions before the Directive; 3 MSs (**Bulgaria, Finland and Italy**) amended their previous legislation to reach the compliance; 2 MSs (**Greece and Spain**) amended their pre-existing legislation even if it was already adequate; and 3 MSs (**Cyprus; Ireland and Malta**) enacted new legislations to achieve compliance. Two special cases remain: **Portugal** has enacted legislation outside the Criminal Code, and **Denmark** is not obliged to transpose the Directive.

Fig. 10: Article 6 of the PIF Directive and national provisions. Absolute number and percentage value of EU Member States. N=25. Year 2024.

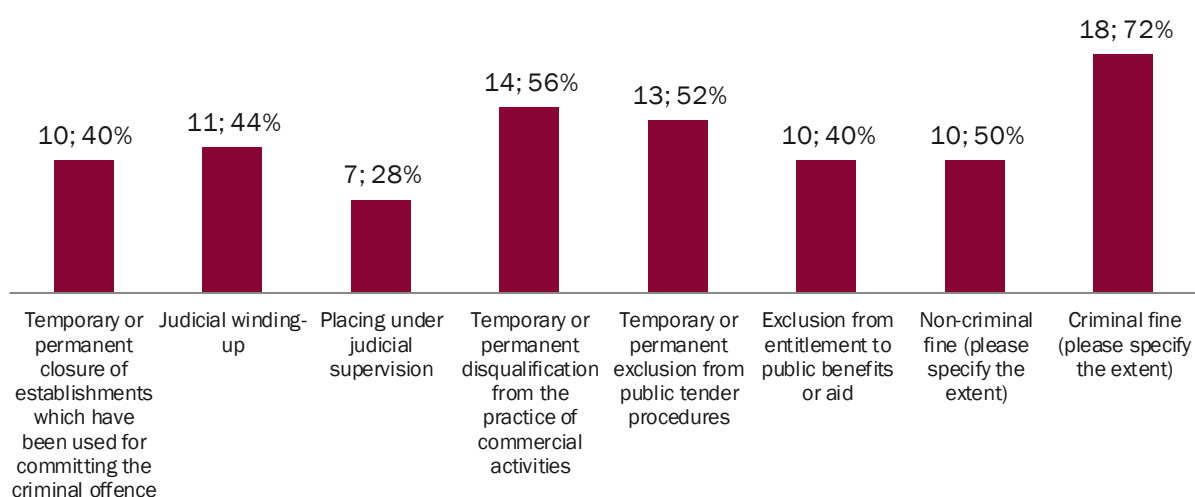


Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

Sanctions with regard to legal persons

Lastly, regarding the sanctions (Fig. 11), these are mainly criminal, although there are also non-criminal ones (administrative or civil). Many of the responding MSs provide for sanctions as indicated in Article 9 of the PIF Directive, either in whole or in part.

Fig. 11: Answers to question 5: “Which of the following sanctions provided for in Article 9 of the PIF Directive in relation to legal persons recognized as responsible under Article 6 are provided for in your national law?”. Absolute number and percentage value of EU Member States. N=25. Year 2024.



Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

4. National criminal law systems and cyber-VAT fraud: similarities and differences between the relevant national legislations of the Member States

The progressive digitalization of economic transactions across the European Union has not only transformed traditional forms of VAT fraud but has also given rise to a new, more complex phenomenon: cyber VAT fraud, as specifically conceptualized and defined in the context of this project.

The aim of this section is to assess whether the existing framework of offences at both the European and national levels is adequate to address emerging trends in cyber VAT fraud or whether **new criminal provisions are necessary** – for example, the introduction of a **specific offense for cyber VAT fraud**.

To explore this, the questionnaire included a **dedicated question** (Q. 6) asking how cyber VAT fraud is addressed under the criminal law of the respondent's country. The focus was on whether such offenses are explicitly recognized and punished. The objective was to examine how cyber VAT fraud—defined by the use of technology or digital tools—is incorporated into the national legal framework. The response options were designed to clarify the various approaches the Member States may adopt in addressing this challenge:

- “No”: Indicates that cyber VAT fraud is not punishable not addressed or punishable under the Member State's criminal law.
- “Yes, there is a specific criminal offense of computer VAT fraud”: suggests the presence of a distinct legal provision explicitly targeting VAT fraud conducted through technological means or within a digital environment.
- “Yes, it is punishable under the offense of VAT fraud (as described in Annex 1)”: Indicates that cyber VAT fraud is encompassed within the broader definition of VAT fraud, without requiring a separate legal classification.
- “Yes, as an aggravating circumstance of VAT fraud”: Signifies that the use of technology to perpetrate VAT fraud is treated as an aggravating factor, resulting in stricter penalties under the existing VAT fraud legislation.
- “Other”: allows for alternative approaches or explanations not covered by the above options.

4.1 National legislations

Austria

Austria considers cyber VAT fraud punishable **under the traditional category of VAT fraud**, due to the free-form nature of this crime.

According to national expert opinions, there is **no necessity for a distinct cyber VAT offense**. Existing European VAT regulations are already **highly complex** and provide robust protection against VAT fraud and safeguard the EU's financial interests. The wide array of provisions and tools in place is deemed sufficient, and introducing additional national laws would only add unnecessary complexity without improving enforcement.

Belgium

In Belgium, cyber VAT fraud is **punishable under the criminal offense of VAT fraud**.

The existing **VAT offenses cover any kind of VAT fraud, regardless of the means** (or *modi operandi*) used, thus including fraud committed by electronic means. Moreover, the Belgian Criminal Code entails a number of specific cyber offenses that may apply in addition to the VAT offense (e.g. cyber forgery (Art. 210bis Criminal Code), hacking (Art. 550bis, §1-§2 Criminal Code) or data interference (Art. 550ter, §3 Criminal Code).

When the technological element concerns the production or forgery of documents, a public prosecutor might also charge the offenders with the production and use of false documents. Several provisions might apply: Article 196 of the Criminal Code, which contains the general criminal offense of forgery, Article 197 of the same Code the general offense of use of forged documents; Article 73bis of the VAT Code which specifically criminalizes the production and use of false documents about VAT fraud, and finally, Article 210bis of the Criminal Code, which criminalizes cyber forgery. As Article 73bis of the VAT Code is the most specific legal provision, it is usually this one that mentioned in the indictment of the public prosecutor when charging a suspect with the forgery in the context of VAT fraud.

The national expert highlighted that, on a different though related point¹²², it is important to highlight that the taxpayers' fiscal liability (i.e. liability with regard to the taxes that are due) is also quite extensive, for example in case of an import from a third country followed by an intracommunity delivery. In such case, the so-called "customs procedure 42" is applied, a mechanism that enables the EU importer to obtain a VAT exemption to avoid pre-financing VAT at the moment of importation. Consequently, the VAT will only be due in the Member State of the destination. While benefiting from the VAT exemption, the importer in the first EU Member State (i.e. the point of entry on EU territory) will often be jointly liable for the whole chain of (subsequent) transactions if it eventually results in a VAT loss in the Member State of destination. If the importer is represented by a tax representative, the latter often shares – or may even carry alone – the burden of VAT liability. Problems arise in particular when adequate proof of onward transport

¹²² Repression is only one enforcement objective, but prevention of fraud and recovery of VAT are equally important objectives in the fight against VAT fraud. Therefore, when reflecting on enhancing criminal liability (whether by introducing new offences or by creating new aggravating circumstances), it should be considered that other liability regimes and enforcement mechanisms are already in place.

outside Belgium (when it constitutes the point of entry into the EU) cannot be presented if it turns out that the consignee of the goods is not the one mentioned on the invoices or transport documents, or if the buyer is a fraudulent actor. Application of customs procedure 42 therefore requires a thorough screening of the parties involved in the chain (following the Know Your Customer (KYC) principle), a rigorous procedure for collecting sufficient proof of transport (which may involve working with an official destination document, which must then be correctly signed off) and clear agreements with clients that provide sufficient guarantees for representatives.

Bulgaria

Cyber VAT fraud is **punishable under the criminal offense of VAT fraud**.

Specifically, it is punishable under the general tax fraud criminal legislation contained in Art. 255 and 255a of the Criminal Code.

Croatia

In Croatia, cyber VAT fraud is **punishable under the major category of the VAT fraud**, as described in Annex 1 and outlined above.

Cyprus

Cyprus is the only MS in the UE that provides for a specific offense of cyber VAT fraud.

In case of a cyber VAT fraud, the sanctions are:

- for physical persons:
 - is subject to a prison sentence not exceeding seven (7) years and/or a fine not exceeding fifty thousand euros (€50,000) and/or both of these penalties, when the loss or benefit exceeds one hundred thousand euros (€100,000);
 - is subject to a prison sentence not exceeding four (4) years and/or a fine not exceeding thirty thousand euros (€30,000) or both of these penalties, when the damage or benefit exceeds ten thousand euros (€ 10,000), but are not greater than one hundred thousand euros (€100,000);
 - is subject to a fine not exceeding ten thousand euros (€10,000) when the loss or benefit is less than ten thousand euros (€10,000).
- for legal persons:
 - is subject to a fine not exceeding 5 hundred thousand euros (€500,000).
- In addition, the court might decide:
 - to order the freezing of its activities;
 - to order a court liquidation;
 - to order the temporary or permanent closure of its establishments.

Czech Republic

On Q. 6 of the questionnaire, Czech Republic answered “**Other**” because the criminal offense of cyber VAT fraud in CZ is punishable as a **general offense of tax evasion** under art. 260 of the Criminal Code as amended by Act No. 315 of 2019 Sb, which implemented the BIP Directive, and not as “traditional” VAT fraud, because there is not a specific crime for it.

The national expert explained that the **Czech Republic handles all tax fraud, including VAT fraud, as a general criminal offence**. He questioned the necessity of creating a specific offense for VAT fraud and found it hard to distinguish VAT fraud from other tax-related crimes. While investigative methods may differ due to the nature of VAT fraud, the criminal consequences should remain consistent across all types of fraud.

Denmark

In Denmark, cyber VAT frauds are **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

Estonia

Even though there were no responses to the questionnaire, it can be considered **based on desk research** that Estonia does not have a specific crime for cyber VAT fraud. Instead, cyber VAT fraud is **covered under broader provisions** related to VAT fraud or tax fraud in general.

Finland

Also in Finland, cyber VAT frauds are **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

France

The answer to Q. 6 “Is cyber VAT fraud punishable under the criminal law of your country?” was “**No** - In the French Criminal Code, there is no specific provision that exclusively addresses cyber VAT fraud.”

This response, while indicating the choice “No,” immediately clarifies that cyber VAT fraud is not disregarded as a crime but rather **lacks an autonomous classification**.

Considering that in France, as explained, there is no specific offense of VAT fraud, but it is punished based on various legislative provisions, it can be assumed that the same approach.

Germany

In Germany, cyber VAT fraud is not an autonomous crime, but it is **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

Greece

In Greece, cyber VAT frauds are **punishable under the “traditional” provision of VAT fraud**. The national expert agrees with most experts: **no specific cyber-VAT fraud offense is needed**. Introducing such an offense would overcomplicate the legal system without adding significant value. The current framework, including **specialised tax crime teams**, is sufficient.

Hungary

In Hungary, cyber VAT frauds are **covered by VAT fraud in general**.

According to the national expert, there is **no need for new criminal offenses or aggravating circumstances unless cyber VAT fraud becomes widespread**. Hungary already has specific offenses for fiscal fraud, so the introduction of cyber VAT fraud as a separate offense only makes sense if the crime is widespread and seriously affects State’s revenue. The national expert highlighted that **digital crimes might require more resources to investigate** but questioned the need for further substantial legislative complexity.

Ireland

In Ireland, cyber VAT fraud is **punishable under the criminal offense of VAT fraud**. There is no specific offence of cyber VAT fraud nor any provision for use of technology as an aggravating circumstance. Cyber VAT fraud would likely be treated in the same manner as non-cyber VAT fraud.

Under the Criminal Law (Theft and Fraud Offences) Act 2001 as amended, there is an offence of “Making gain or causing loss by deception” (section 6). This is a broadly worded provision that could be used in VAT fraud contexts and carries a maximum sentence of 5 years imprisonment. Notably, there is also a similar offense of “Unlawful use of a computer” (section 9) which carries a maximum sentence of 10 years. This is perhaps the best example under Irish Criminal Law of how the use of technology could be seen as akin to an aggravating circumstance.

The national expert concurs with others on the **unnecessary introduction of specific offenses**. Existing VAT-related offences are sufficient.

Italy

In Italy, there is **no specific offense for cyber VAT fraud either**. Instead, it is included within the broader category of VAT fraud, as VAT fraud is considered a crime with a free-form structure.

For the national expert, there is **no need for specific Cyber-VAT fraud provisions**, because fraud increasingly involves digital tools, but this is **just an evolution of traditional fraud**. The difficulty lies in identifying the perpetrators, not the method of the fraud.

Also in this case, the expert highlighted the importance of improving the investigative tools on this cybercrime, as for cybercrimes in general. In the fight against cybercrime, or more generally against crimes committed through technology, it now seems that the procedural aspect of criminal law is more significant than substantive criminal law. So, it is **more important to develop new tools or clarify how they should be applied, rather than creating new legal provisions**.

Latvia

In Latvia, cyber VAT fraud is **not an autonomous crime**, but it is **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

Lithuania

The same for Lithuania, where cyber VAT frauds are **covered by VAT fraud in general**, as described in Annex 1 and outlined above.

Luxembourg

Cyber VAT fraud is **punishable under the criminal offense of VAT fraud** (as described in Annex 1).

The national expert highlighted that **some of the features of a cyber VAT fraud may even lead to a requalification** from mere “tax fraud” to “*escroquerie fiscale*”, **with aggravated penal sanctions**: Art. 80 of the Lux VAT law establishes that: “If the perpetrator has systematically used fraudulent tactics with the intention of concealing relevant facts from the administration or in persuading it of incorrect facts and the fraud so committed or attempted relates, per reporting period, to a significant amount of value added tax evaded or refund improperly obtained either in absolute amount or in relation to the value added tax due per reporting or refund period effectively due per declaration period, the perpetrator will be punished, for tax fraud (“*escroquerie fiscale*”), by imprisonment from one month to five years and a fine of 25,000 euros in an amount representing ten times the value added tax evaded or the refund wrongly obtained”.

Malta

In Malta, cyber VAT fraud is not an autonomous crime, but it is **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

The Netherlands

In The Netherlands, cyber VAT fraud is not an autonomous crime, but it is **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

The national expert highlighted that in the Netherlands, **all VAT operations are reported electronically**, making all VAT fraud digital by definition.

There is **no need for a specific offense for cyber VAT fraud**, as crimes are already treated in a technology-neutral manner. **An aggravating circumstance for the use of digital means would not add significant value either.**

Poland

In Poland, cyber VAT fraud is not an autonomous crime, but it is **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

According to the national expert, the **current VAT fraud laws are adequate**. Poland uses a combination of administrative and criminal sanctions to fight VAT fraud and has seen success in reducing the VAT gap. As cyber fraud becomes more common, adjustments may be needed, but for now, traditional methods are effective.

Portugal

In Portugal, cyber VAT fraud is not an autonomous crime, but it is **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

Romania

Cyber VAT frauds are **punishable under the general offence of VAT fraud**, as defined in Annex 1 and above.

Also, for the Romanian national expert, there is **no need for a specific cyber VAT offense**. Romania has **harsh penalties for VAT fraud, including up to 16 years in prison**. The actual national focus is on reducing the VAT gap, and electronic reporting (e.g., e-invoicing) already covers the technological aspects. For the national expert, the current legal framework is comprehensive enough.

Slovakia

The answer to Q. 6 of the questionnaire “Is cyber VAT fraud punishable under the criminal law of your country?” was “**No**”.

Nevertheless, considering what has been described in the previous section, it is understood that the response does not intend to disregard cyber VAT fraud as a crime, but simply highlights the **absence of a specific offense**, with such fraud being considered **part of the broader category**, especially given the free-form nature of VAT fraud as a crime.

Slovenia

Even though there were no responses to the questionnaire, it can be considered based on **desk research** that Slovenia does not have a specific crime for cyber VAT fraud. VAT fraud, including cyber VAT fraud, is typically addressed **under the broader framework of tax fraud offenses in the country**. These offenses are part of the general criminal provisions regarding fraud and tax evasion.

Spain

In Spain, cyber VAT fraud is not an autonomous crime, but it is **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

Also according to the Spanish national expert, there is **no need for a specific offense**. Cyber-VAT fraud is a natural evolution of VAT fraud, and the use of technology should not change the classification of the crime. Spain **already has aggravated offences for using shell companies**, regardless of whether technology is involved. The existing general tax fraud regulations cover all methods, including electronic means. The main need is for **specialised professionals and technical resources** rather than new legislation.

Sweden

In Sweden, cyber VAT fraud is not an autonomous crime, but it is **punishable under the major category of VAT fraud**, as described in Annex 1 and outlined above.

4.2 Considerations concerning a possible autonomous offence

As mentioned, **not all MSs provide for an autonomous offense of VAT fraud, as in many cases it is included within the broader category of tax fraud or tax evasion**. Therefore, a significant number of specific provisions for cyber VAT fraud was not expected, especially considering that, although widespread, it has not yet been studied extensively in a specific manner. Moreover, in most cases, as observed, VAT fraud is **considered a free-form offense**, or – even when a precise list of conducts is provided – these actions are broadly defined. Consequently, it was expected that the cyber element **could be easily encompassed within these existing provisions**.

After collecting the responses to the questionnaire, this topic became a **key point of discussion during the first online focus group**, which aimed, among other objectives, to explore **effective options for the criminalization of cyber VAT fraud**. Participants were asked to share their views on whether there is a need for a specific criminal offense for VAT fraud in the digital space and, for those who did not consider this necessary, whether it is sufficient to address it under the broader category of “traditional” VAT fraud, or if it should be treated as an aggravating circumstance within the existing VAT fraud framework. Minutes from the meeting were recorded, and the insights and discussions from the session were incorporated into this study.

The majority of MSs (21) consider cyber VAT fraud punishable under the traditional category of VAT fraud, due to the free-form nature of this crime.

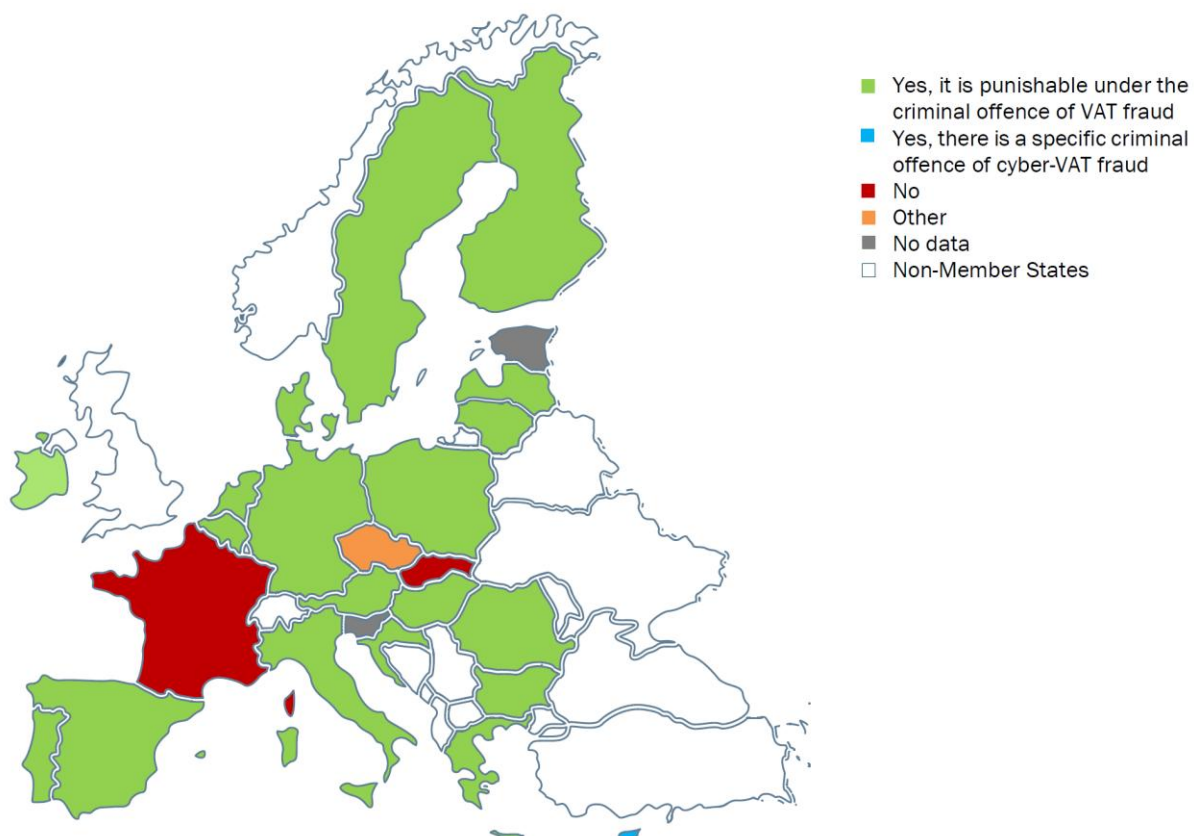
According to the study results, there is no need to introduce a specific offense for Cyber-VAT fraud: this is an evolution of traditional VAT fraud and it can be adequately addressed under existing legal frameworks. There was also broad agreement that specialized investigative units and enhanced technical resources would be more effective than creating new offenses or treating cyber elements as aggravating circumstances.

Even in this type of cybercrime, as with others that can also be committed "offline", where technological elements are configurable as modes of conduct or specific components (so-called cybercrime in a broad sense), it is much more important to regulate the investigation phase, specifically the collection of evidence. Therefore, investigative tools suitable for managing the technological elements of criminal conduct are needed, tools that assist with real-time monitoring and analyze – possibly with the help of artificial intelligence, in full respect of procedural safeguards and with proper balancing of the various fundamental rights at stake – of the large volume of data being collected.

Cyprus is unique in having legislated a specific offense for cyber VAT fraud, with graduated penalties for both natural and legal persons depending on the financial damage involved. Some jurisdictions, while not having a separate offense, implicitly consider digital means as aggravating factors (as for instance, in Ireland: “Unlawful use of a computer” can result in up to 10 years imprisonment, potentially applying to cyber VAT fraud contexts; in Luxembourg: “Escroquerie fiscale” allows for enhanced penalties where digital manipulation is systematic and deceptive).

While criminal enforcement remains central to the fight against VAT and cyber VAT fraud, not all Member States place equal emphasis on the complementary roles of administrative and civil liability. Belgium stands out in this regard, offering a more nuanced and multidimensional enforcement framework. In particular, it underscores the administrative liability of tax representatives involved in cross-border transactions and highlights the significance of customs mechanisms, such as Procedure 42, which allows for VAT exemption upon importation under specific conditions. This procedure requires careful documentation and due diligence, including proof of intra-EU transport and application of "Know Your Customer" (KYC) principles. Failure to comply can trigger administrative or even civil liability for both importers and their representatives, in addition to potential criminal charges. This integrated approach, which blends criminal, administrative, and civil accountability, aims not only to punish but also to prevent and recover VAT losses. However, such a comprehensive liability framework is not uniformly implemented across the EU. In many other Member States, enforcement still leans heavily on criminal prosecution, with less structured mechanisms for assigning administrative or civil liability in complex VAT fraud schemes. As a result, the level of deterrence, prevention, and financial recovery varies considerably depending on national legal and procedural systems.

Fig. 12: Answer to question 6: “Is cyber VAT fraud punishable under the criminal law of your country?” EU Member States. N=25. Year 2024.



Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

5. Combating cyber-VAT fraud and criminal investigations: similarities and differences between the relevant national legislations of the Member States

This section provides a comprehensive analysis of VAT fraud and cyber VAT fraud from a **criminal procedural perspective**, focusing on how investigative powers and tools are used by police, judicial, and tax authorities across EU Member States. It evaluates not only the effectiveness and adequacy of these measures but also whether disparities between national systems might undermine the EU-wide response to VAT fraud.

A central theme is the role of EU institutions—including OLAF, the European Public Prosecutor's Office (EPPO), Eurojust, Europol, and the European Court of Auditors—in supporting cross-border cooperation. For example, in 2023, Eurojust supported almost 300 PIF-related cases, and the EPPO was involved in a growing number of joint investigations (Eurojust, 2023). These bodies help coordinate efforts and facilitate the exchange of information across jurisdictions.

5.1 Investigative tools against cyber-VAT fraud

According to the study, the majority of MSs do not have dedicated tools for cyber VAT fraud but instead rely on general fraud investigation methods—such as data analytics, routine audits, search and seizure operations, interviews, surveillance, and international collaboration. Tools like open-source intelligence (OSINT), AI-based detection, lawful hacking and digital forensic techniques are becoming more relevant, though adoption varies widely (as for instance in Malta). In any case, a clear and precise regulation governing the use of artificial intelligence tools is indispensable. Such regulation should distinguish between the different phases of the investigation—whether pre-investigative, at the preventive stage, or post-initiation of criminal proceedings—and must take into account both the evolving European legal framework on the subject and the necessary balancing of the fundamental rights at stake.

Despite this reliance on traditional methods, experts consistently highlighted the need for:

- **Specialised training for investigators in digital and cybercrime** (e.g., Portugal, Hungary, Czech Republic);
- **Enhanced inter-agency cooperation** (e.g., Greece, Bulgaria);
- **Greater use of AI and big data** (e.g., Portugal, Italy);
- **Legal reforms to extend investigation timeframes and clarify offenses** (e.g., France, Spain);
- **Improved data integration and centralized databases** (e.g., Romania, Croatia);
- **Stronger international coordination, including through EU instruments like the European Investigation Order.**

Moreover, some MSs experts pointed to the need for new structures, such as specialized fiscal police or dedicated prosecutorial units; for example, the national expert for Bulgaria highlighted

how a specialised unit for ‘Tax Control’ had been set up within the National Revenue Agency, designed to promptly and effectively conduct criminal proceedings against financial fraud, with a particular focus on VAT fraud.

Others experts, like Malta’s one, emphasized the importance of aligning criminal and administrative sanctions. Some countries (notably France, Spain, and Latvia) advocate updating legislation to clearly define VAT fraud offenses and penalties and to improve procedural efficiency.

Tab. 1: Answers to question 7: “On which investigative tools/measures law enforcement authorities in your country can rely on for investigative purposes?”. EU Member States. N=25. Year 2024.

	Data analysis and information sharing	Audits and inspections	Search and seizure	Interviews, audits and surveillance	Collaboration with other agencies	Coercive measures
AT			X			
BE	X				X	
BG		X	X	X		
CY	X	X	X	X	X	X
CZ	X				X	
DE		X	X	X	X	
DK		X				
ES	X				X	
FI	X	X	X	X	X	
FR	X	X		X	X	
GR	X	X		X	X	
HR	X			X	X	
HU	X	X	X	X	X	
IE	X	X	X	X	X	
IT	X	X	X	X	X	
LT		X	X	X	X	X
LU	X	X			X	
LV	X				X	
MT	X	X	X			X
NL	X		X	X	X	
PL	X	X	X	X	X	
PT					X	
RO	X	X				
SE			X			X
SK	X				X	

Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

As a general perception, it can be observed in all European countries that the **investigative tools and measures used for general VAT fraud also apply to cyber VAT fraud**, thus **specific tools tailored for cyber VAT fraud are very rare**: several countries (Malta, Hungary, Italy, Ireland, Lithuania, Bulgaria, Spain, Slovakia, Romania, Luxembourg, Czech Republic; and Belgium) report that there are **no specific tools designed for cyber VAT fraud**, indicating a reliance on general fraud investigation tools. **Latvia** points out the continuous commitment to advance expertise and share best practices among jurisdictions, managing to adapt “traditional” strategies to nowadays phenomena.

Some of the tools indicated in the table are related only to the pre-trial investigations, as for instance audits and inspections and collaboration with o the authorities in Lithuania ¹²³.

In summary, while many countries rely on traditional investigative tools adapted for cyber contexts, the **question 9** of the questionnaire (“*How could the national criminal procedure be improved to better combat VAT fraud in your country?*”) and **10** (“*How could the national criminal procedure be improved to better combat cyber VAT fraud in your country?*”) highlights how there is a clear need for **specialised training**: Portugal, for example, underlines the importance of specialised training for investigators in cybercrime and fraud, indicating ongoing collaboration with European Union agencies for law enforcement training - and technological advancements to effectively combat cyber VAT fraud.

Finally, **cooperation at the EU level** also plays a significant role in addressing the transnational nature of these crimes; the implementation of EU directives, such as the European Investigation Order and reporting obligations for cross-border money transfers (as seen in the Czech Republic), illustrates a coordinated approach across Member States to enhance the effectiveness of investigations.

Article 11 of the PIF Directive requests that each MSs take the necessary measures to establish its jurisdiction over the criminal offences where:

- the criminal offense is committed in whole or in part within its territory; or
- the offender is one of its nationals.

All the responding MSs – except for Cyprus - apply their own jurisdiction based on the principle of territoriality. Most of all apply also the personality principle (20 out of 24).

Article 11 also allows for the possibility of establishing specific cases and exceptions, albeit within certain limits and with the obligation to inform the Commission in the event of adopting specific jurisdiction-related decisions.

The **limitation period** is the legally defined time frame within which authorities can initiate legal proceedings against an offender after a crime has been committed. Once this period expires, prosecution is no longer possible, meaning the offender cannot be legally charged or tried for the crime. VAT fraud and cyber VAT fraud, especially in complex or cross-border cases, often involve

¹²³ More in detail, the Code of Criminal procedure of Lithuania did not mention directly “audit and inspections”, but the me result can be achieve by an expert report or specialisti conclusions provided for in the Code after conducting an expert or specialist study on variuous, inter alia, financial-economic issues. Meanwhile, collaboration between agencies durino eh pre-trial investigation stage (under the Code of Criminal procedure) is possible by forming a joint investigative team by the decision of the prosecutor.

sophisticated schemes, multiple entities, and digital transactions that make investigations lengthy and difficult. A longer limitation period is crucial for several reasons:

1. **Complex Investigations** – VAT fraud cases often require in-depth financial analysis, cross-border cooperation, and digital forensics, which can take years to uncover and prove. A short limitation period could allow criminals to escape justice before authorities complete their investigations.
2. **International Cooperation** – Many VAT fraud schemes, such as **carousel fraud (MTIC fraud)**, involve multiple countries. Legal cooperation between jurisdictions can take time, and a longer limitation period ensures that international legal requests (e.g., extradition, data-sharing) can be processed effectively.
3. **Deterrence** – Fraudsters might engage in long-term tax evasion schemes, knowing that if they remain undetected for a few years, they could avoid prosecution. A longer limitation period increases the risk of being caught and penalized, discouraging potential offenders.
4. **Recovery of Damages** – A longer timeframe allows authorities to track and recover illicit gains from fraudulent activities, ensuring that stolen VAT revenue can be reclaimed and reinvested into public funds.
5. **Adaptation to New Fraud Tactics** – Fraud schemes evolve with new technologies and loopholes. Investigators need time to trace hidden transactions, decrypt data, and follow financial trails that might only become evident after several years.

Under **Article 12 of the PIF (Protection of Financial Interests) Directive**, EU Member States are required to have a limitation period of at least **five years** for serious VAT fraud cases, ensuring that authorities have enough time to prosecute offenders and recover stolen funds.

The **vast majority of EU Member States comply with the provisions of Article 12 of the PIF Directive**. Some countries have even longer periods, depending on the severity of the offense.

5.2 National legislations

Austria

First, the national expert emphasized the importance of **distinguishing between tax investigations and criminal investigations**. Regarding criminal investigations, all measures outlined in the **general Criminal Procedure Code** are applicable, including **surveillance, wiretapping, searches of dwellings, and the freezing and seizure of evidence such as documents and data**. Interceptions are permitted when the fraud is deemed serious — i.e. when it exceeds a specific threshold or is committed by an organized criminal group.

In terms of **tax investigations**, **significant organizational measures have been implemented in recent years**. Notably, the results Tax Investigation Authority established a specialized "Umsatzsteuer-Betrugsbekämpfungs-Competence-Center (USt-BBCC)", an **Anti-VAT Fraud Competence Center**. Tax authorities also employ **AI-based electronic analysis tools**.

The expert also noted that **Austria uses both general and specialized investigative measures in combating VAT fraud and cyber VAT fraud**, with a strong emphasis on **data analysis and inter-agency collaboration**. A dedicated anti-fraud unit within the Ministry of Finance **automatically scans all data to identify risks**. If no risks are detected—not only regarding VAT fraud but also broader tax

fraud—the taxpayer’s tax return is processed and returned the following day. If risks are identified, a more thorough investigation is conducted. The expert further mentioned that the **Artificial Intelligence Act is underway** and will address sensitive personal data, imposing restrictions on its use. This will introduce additional standards for applying digital data analysis. Considering the AI Act’s risk-based differentiation, its provisions for high-risk AI systems and data processing can be inferred. This includes **stringent rules to ensure transparency, accountability, and the protection of taxpayers' rights**.

Regarding **jurisdiction**, Austria asserts its jurisdiction over financial offenses committed within its borders. An act is deemed to have been "committed" on Austrian territory if either the action or the result occurs there, or if it should have occurred according to the perpetrator's plan. Additionally, if the financial offense is committed in the EU's customs territory but discovered in Austria, or if it is committed against an Austrian tax authority official working abroad based on an international treaty, it is considered to have been committed in Austria under § 5 para. 2 FinStrG¹²⁴. The personality principle applies as well, meaning that if an Austrian national commits fraud, Austria retains jurisdiction.

Austria is **compliant with Article 12 of the PIF Directive**, which specifies a **minimum limitation period of five years** for the criminal offense of VAT fraud. This aligns with Austria’s general limitation period of five years for the enforcement of tax offense convictions. Similar to most of the respondents (including Belgium, Croatia, Cyprus, Czech Republic, Hungary, Ireland, Poland, Romania, Sweden, and the Netherlands), Austria specifies that penalties for VAT fraud can be enforced for at least five years from the date of the final conviction, whether the penalty involves more than one year of imprisonment or a sentence for a crime punishable by up to four years of imprisonment.

Belgium

In Belgium, as in other EU Member States, the investigative powers of the public prosecutor's office are primarily established by the **Code of Criminal Procedure (CCP)**. These powers are not specific to VAT fraud but apply to investigations of all offenses. However, **specific investigative powers related to VAT fraud are detailed in the VAT Code** (Art. 59 and following¹²⁵). These powers fall under

¹²⁴ Article 5 FinStrG:

(1) A financial offense is only punishable if it has been committed within the country.

(2) A financial offense is considered to have been committed within the country if the perpetrator acted within the country or should have acted within the country, or if the result corresponding to the offense occurred within the country or, according to the perpetrator's expectation, should have occurred there. If the financial offense is not committed within the country, but within the customs territory of the European Union, and is discovered in the country, or if it is committed by an Austrian national abroad, or if it is committed against an authority of a tax administration acting abroad based on an international treaty, it shall be considered as committed within the country.

(3) No one may be extradited to a foreign country for a financial offense, and a punishment imposed by a foreign authority for such an offense may not be enforced in the country, unless otherwise provided in international treaties or federal laws.

¹²⁵ Art. 59 VAT Code:

(1) The administration is authorized to provide proof in accordance with common legal rules and by all means of common law, including witnesses and presumptions, but excluding oaths. Additionally, it may rely on the official reports of the Federal Public Service for Finance to demonstrate any violation or abusive practice of the provisions of this Code or its implementing regulations, as well as any fact that establishes or contributes to establishing the tax liability or a penalty. The official reports are considered valid evidence unless proven otherwise.

the jurisdiction of the VAT administration rather than the public prosecutor's office and are employed in administrative investigations.

The VAT administration lacks the authority to initiate criminal prosecutions. As highlighted by the national expert, if a case warrants criminal proceedings (e.g., in cases of serious fraud), the administration must notify the public prosecutor's office, in accordance with Article 29, §§ 2-3 of the CCP¹²⁶. Once the public prosecutor's office assumes the case, the remaining investigation is governed by the CCP's provisions for criminal investigations. **According to financial news reports, the VAT administration employs data mining to detect fraud, using both open-source data and taxpayer-submitted information** (e.g., VAT client listings, declarations, European Community sales lists, etc.) filed via the Ministry of Finance's platform, "MyMinfin." They also **cross-check data with other authorities, such as customs**. However, the specifics of how data mining and AI tools are utilized remain undisclosed.

The national expert emphasized the importance of differentiating between two forms of digitalization:

- digitalization of **tax returns** — converting analog documents into digital formats and streamlining business processes using digital technology;
- digitalization of **investigations** — using digital investigative tools to enhance detection and enforcement efforts.

Both areas require improvement to effectively address EU-wide cyber VAT fraud.

The VAT administration receives extensive taxpayer data via digital tax returns but lacks sufficient resources and tools to efficiently analyze this data to identify fraud patterns. While a digital platform exists, the process of collecting additional documentation during investigations remains cumbersome. Currently, businesses under investigation are asked to provide VAT-related

(2) Without prejudice to the other means of proof provided for in paragraph 1, the official designated by the King or the taxpayer has the right to request an expert assessment to determine the normal value of goods and services referred to in Article 36, paragraphs 1 and 2.

This right also applies to the goods referred to in Article 19, paragraph 2, point 1, when they concern the construction of a building.

The King establishes the procedure for the expert assessment. He determines the timeframe within which this procedure must be initiated and specifies the person responsible for bearing the costs.

[...]

¹²⁶ Art. 29 §§ 2-3 CCP

§ 2. Officials of the General Administration of Taxation, the General Administration of Collection and Recovery, the General Administration of Property Documentation, the General Administration of Special Tax Inspection, or the competent official in cases of regional or local taxation may not, without the authorization of the general advisor to whom they report or an equivalent official, bring to the attention of the Public Prosecutor facts that are criminally punishable under tax laws and the regulations enacted for their enforcement.

§ 3. Without prejudice to the application of paragraph 2, the general advisor of the General Administration of Taxation, the General Administration of Collection and Recovery, the General Administration of Property Documentation, and the General Administration of Special Tax Inspection, or the official they designate, or the competent official in cases of regional or local taxation, shall report to the Public Prosecutor any facts that, upon examination, reveal serious indications of serious tax fraud, whether organized or not, constituting criminal offenses under tax laws and the regulations enacted for their enforcement.

The Public Prosecutor shall consult with the officials referred to in the first paragraph within one month of receiving the report. He may invite the competent police services to participate in this consultation. [7 The consultation may also take place at the initiative of the Public Prosecutor.]7

Based on the consultation, the Public Prosecutor decides which facts [7 ...]7 will lead to the initiation of public prosecution and informs the competent general advisor or the competent official in cases of regional or local taxation in writing, no later than three months after the initial report mentioned in the first paragraph.

documentation (e.g., records of their 20 largest clients) in diverse digital formats (e.g., screenshots, PDFs), complicating analysis. **Standardizing and streamlining this process would significantly enhance investigative efficiency together with the use of AI tools.**

The expert further advocated for **real-time identification tools for economic operators**, preferably based on blockchain technology. Such tools could enable VAT authorities and businesses to verify the legitimacy and activity status of economic operators during transactions (e.g., detecting shell companies or VAT identity theft). Existing systems like the VAT Information Exchange System (VIES) and the Central Databases of Undertakings lack real-time data and are therefore insufficient. A real-time EU-wide identification platform would benefit both authorities and businesses by reducing risks of fraud and joint fiscal liability.

The Belgian VAT administration is addressing some challenges by inspecting newly established e-commerce businesses within their first six months of operation to promote VAT compliance. However, this approach addresses only part of the broader need for real-time tools and **proactive measures**.

With regards to the **jurisdiction**, Belgium applies the **principle of territoriality**, supported by the “objective ubiquity theory” developed by the Court of Cassation. This theory grants Belgian criminal law jurisdiction if any material element of the offense occurs on Belgian territory, irrespective of the offender's nationality. Additionally, if several offenses are part of a broader criminal plan, the jurisdiction covers all related offenses if any material element occurs in Belgium. The intent behind the offense is irrelevant to establishing jurisdiction.

If the material element, or part of it, of one of these offenses can be located in Belgium, the whole set of offenses will be considered as falling within the jurisdiction of the Belgian courts.

The **principle of personality also applies**, granting Belgian jurisdiction if the offender is a Belgian citizen or resides habitually in Belgium. This principle extends to officials acting in their capacity under staff regulations at the time of the offense.

Key provisions include:

- Belgian nationals or residents who commit offenses abroad can be prosecuted if the act is punishable in the country where it occurred (Art. 6, § 1 PTCCP, as amended by the Act of 9 April 2024)¹²⁷;

¹²⁷ Article 6 § 1 PTCCP:

Subject to the application of Articles 7 to 11, any Belgian citizen or any person habitually residing in the territory of the Kingdom who, outside the territory of the Kingdom, has committed an act classified as a crime or offense under Belgian law may be prosecuted in Belgium if the act is punishable under the legislation of the country where it was committed.

- offenders cannot be prosecuted in Belgium if they have already been acquitted, served a sentence, or if enforcement is time-barred under the principle of ne bis in idem, except in cases of fair trial violations (Art. 14¹²⁸ and 14/1, para. 1 PTCP¹²⁹);

¹²⁸ Article 14 PTCCP:

Any person who commits, outside the territory of the Kingdom, one of the offenses referred to in Articles 347bis, 393 to 397, and 475 of the Penal Code against a person who, at the time of the act, is Belgian, may be prosecuted in Belgium if the act is punishable under the legislation of the country where it was committed by a penalty with a maximum exceeding five years of deprivation of liberty.

If the suspect is not found in Belgium, prosecution, including the investigation, can only be initiated at the request of the Federal Prosecutor or the Public Prosecutor, who assesses any potential complaints.

When presented with a complaint under paragraph 2, the Federal Prosecutor or the Public Prosecutor shall instruct the investigating judge to proceed with the investigation of the complaint, unless:

1° The complaint is manifestly unfounded; or

2° The facts alleged in the complaint do not constitute one of the offenses referred to in Articles 347bis, 393 to 397, and 475 of the Penal Code; or

3° A valid public prosecution cannot arise from the complaint; or

4° From the specific circumstances of the case, it appears that, in the interest of proper administration of justice and in compliance with Belgium's international obligations, the case should be brought either before international jurisdictions, or the jurisdiction of the place where the acts were committed, or the jurisdiction of the state of which the perpetrator is a national or where the perpetrator can be located, provided that such jurisdiction meets the standards of independence, impartiality, and fairness, as can be inferred, in particular, from relevant international commitments binding Belgium and that state.

If the Federal Prosecutor or the Prosecutor General believes that one or more of the conditions referred to in paragraph 3, 1°, 2°, and 3°, are met, they shall request the chamber of indictments to declare, as appropriate, that there are no grounds for prosecution or that the public prosecution is inadmissible. Only the Federal Prosecutor or the Prosecutor General is heard.

If the chamber of indictments finds that none of the conditions referred to in paragraph 3, 1°, 2°, and 3°, are met, it shall designate the territorially competent investigating judge and specify the facts to be investigated.

Proceedings will then follow standard legal procedure.

The Federal Prosecutor or the Prosecutor General has the right to lodge an appeal in cassation against decisions rendered under paragraphs 4 and 5. In all cases, this appeal must be filed within fifteen days of the ruling.

In the case referred to in paragraph 3, 4°, the Federal Prosecutor or the Public Prosecutor shall close the case without further action and notify the Central Authority established by Article 2, fourth indent, of the Law of March 29, 2004, on cooperation with the International Criminal Court and international criminal tribunals.

This decision to close the case is not subject to appeal.

¹²⁹ Article 14/1 PTCCP:

Any person who commits, outside the territory of the Kingdom, one of the offenses referred to in Book II, Title I ter, of the Penal Code against a person who, at the time of the acts, is a Belgian citizen or against a Belgian institution, may be prosecuted in Belgium.

If the suspect is not found in Belgium, prosecution, including the investigation, can only be initiated at the request of the Federal Prosecutor or the Public Prosecutor, who evaluates any potential complaints.

When presented with a complaint under paragraph 2, the Federal Prosecutor or the Public Prosecutor shall instruct the investigating judge to process the complaint unless:

1° The complaint is manifestly unfounded; or

2° The facts alleged in the complaint do not correspond to a classification of the offenses referred to in Book II, Title I ter, of the Penal Code; or

3° A valid public prosecution cannot arise from the complaint; or

4° From the specific circumstances of the case, it appears that, in the interest of proper administration of justice and in compliance with Belgium's international obligations, the case should be brought either before international jurisdictions, the jurisdiction of the place where the acts were committed, or the jurisdiction of the state of which the perpetrator is a national or where the perpetrator can be located, provided that such jurisdiction meets the standards of independence, impartiality, and fairness, as can be inferred, in particular, from relevant international commitments binding Belgium and that state.

If the Federal Prosecutor or the Prosecutor General believes that one or more of the conditions referred to in paragraph 3, 1°, 2°, and 3°, are met, they shall request the chamber of indictments to declare, as

- if the offense is committed against a foreigner, the prosecution requires the foreign victim to file a complaint or for the foreign state to notify Belgian authorities (Art. 6, § 2 PTCCP¹³⁰). It must be noticed that, in VAT offenses, the victim is typically a state, which is unlikely to defer jurisdiction to Belgium.

Additionally, prosecution is only possible if the offender is found in Belgium (Art. 6, § 3 PTCCP¹³¹). Co-perpetrators and accomplices can also be prosecuted alongside or separately from the main offender (Art. 14/11 PTCCP¹³²).

Belgium prosecutes offenses committed for the benefit of legal entities established within its territory. Such cases fall under **corporate criminal liability** (Art. 5¹³³, para. 1 Criminal Code), provided the required mens rea can be established. The recent amendment to Art. 7, § 1 PTCCP¹³⁴ ensures that even if all elements cannot be proven for the legal entity, a natural person committing an offense for its benefit can still be prosecuted. This, too, requires the offender to be located in Belgium (Art. 7, § 2 PTCCP¹³⁵).

appropriate, that there are no grounds for prosecution or that the public prosecution is inadmissible. Only the Federal Prosecutor or the Prosecutor General is heard.

If the chamber of indictments finds that none of the conditions referred to in paragraph 3, 1°, 2°, and 3°, are met, it shall designate the territorially competent investigating judge and specify the facts to be investigated. If the request referred to in paragraph 4 comes from the Federal Prosecutor, it shall refer the case to the dean of investigating judges mentioned in Article 47duodecies, § 3, of the Code of Criminal Procedure.

Proceedings will then follow standard legal procedure.

The Federal Prosecutor or the Prosecutor General has the right to lodge an appeal in cassation against decisions rendered under paragraphs 4 and 5. In all cases, this appeal must be filed within fifteen days of the ruling.

In the case referred to in paragraph 3, 4°, the Federal Prosecutor or the Public Prosecutor shall close the case without further action and notify their decision to the Central Authority established under Article 2, fourth indent, of the Law of March 29, 2004, concerning cooperation with the International Criminal Court and international criminal tribunals. This decision to close the case is not subject to appeal.

¹³⁰ Article 6 § 2 PTCCP:

If the offense was committed against a foreigner, prosecution may only take place upon the request of the public prosecutor and must also be preceded by a complaint from the offended foreigner or their family, or by an official notification given to the Belgian authorities by the authorities of the country where the offense was committed.

In the event that the offense was committed, during wartime, against a national of a country allied with Belgium within the meaning of Article 117, paragraph 2, of the Penal Code, the official notification may also be given by the authorities of the country of which the foreigner is or was a national.

¹³¹ Article 6 § 3 PTCCP:

The prosecution of a Belgian will only take place if they are found in Belgium, except when the offense was committed during wartime or if it concerns an offense referred to in Articles 347bis, 393 to 397, and 475 of the Penal Code.

The prosecution of a foreigner will only take place if they are found in Belgium, except if it concerns an offense referred to in Articles 347bis, 393 to 397, and 475 of the Penal Code, or, when the offense was committed during wartime, if they are found in enemy territory or if their extradition can be obtained.

¹³² Article 14/11 PTCCP:

The foreigner who is a co-perpetrator or accomplice of a crime committed outside the territory of the Kingdom by a Belgian may be prosecuted in Belgium, jointly with the suspected Belgian or after the conviction of the latter.

¹³³ See footnote no. 18.

¹³⁴ Article 7 § 1 PTCCP:

Any person who commits an offense on behalf of a legal entity whose registered office is located on Belgian territory may be prosecuted in Belgium.

¹³⁵ Article 7 § 2 PTCCP:

The prosecution of a Belgian national will only take place if they are found in Belgium, unless the offense was committed during wartime.

Finally, Belgium **complies with Article 12 of the PIF Directive**, which mandates a minimum **five-year limitation period for VAT fraud**. The Act of 9 April 2024 extended the limitation period for misdemeanors to **10 years** (from five). Under the new law, specifically Article 21¹³⁶, the limitation period applies only during the pretrial stage. Once the case is formally brought to trial, the limitation period stops, allowing proceedings to continue without time-barred risks. The only requirement is adherence to reasonable trial timelines.

Bulgaria

According to Bulgarian criminal procedure, a **full range of investigative tools is employed in the fight against VAT fraud**. These include suspect and witness interrogations, inspections, expert analyses, searches, and seizures, alongside the use of special investigative techniques.

The most frequently used and effective tools include written evidence of an authentic nature — whether in paper or electronic format — that complies with regulatory requirements. Examples include documents certifying cash flows, tender contracts, and acts of acceptance. Additionally, interrogations of experts, employees, and consultants as witnesses, as well as searches and seizures, particularly of computer data and configurations (including on the premises of consultancy companies), play a crucial role in uncovering VAT fraud schemes.

According to the national expert, while these tools are effective, there are areas where significant improvements could be made. These include:

- **enhanced training** for specialized staff to ensure they possess the necessary skills and knowledge to handle increasingly sophisticated fraud cases.
- **establishing new specialized structures** to focus exclusively on combating VAT fraud and improving overall efficiency.
- **strengthening international cooperation** and collaboration with other competent authorities, recognizing that VAT fraud often involves cross-border elements.
- **incorporating AI technologies** to analyze complex datasets, detect patterns, and identify fraudulent activities more effectively.
- **raising awareness among stakeholders**, including businesses and economic operators, to enhance vigilance and compliance in this area.

According to the national expert, by addressing these priorities, Bulgaria can significantly strengthen its capacity to combat VAT fraud and improve the overall effectiveness of its investigative efforts.

In Bulgaria, both the **principles of territoriality and personality** are applied in determining **jurisdiction**. This means that Bulgarian criminal law applies to crimes committed on Bulgarian

The prosecution of a foreign national will only take place if they are found in Belgium, or, if the offense was committed during wartime, if they are found in an enemy country or if their extradition can be obtained.

¹³⁶ Article 21 § 1 PTCCP:

Except in the cases referred to in Article 21bis, criminal proceedings shall be time-barred, counting from the day on which the offence was committed, by the lapse of 30 years, 20 years, 15 years, 10 years or one year, depending on whether the offence constitutes a crime punishable by life imprisonment, a crime punishable by more than 20 years to 30 years of imprisonment, a crime punishable by more than 5 years to 20 years of imprisonment or less, a misdemeanor or a petty offence.
[...].

territory, as well as to crimes committed by Bulgarian citizens abroad, provided this is stipulated in an international agreement to which Bulgaria is a party.

Under Bulgarian law, no citizen of the Republic of Bulgaria can be extradited to another state or an international court for prosecution unless such extradition is explicitly provided for in an international agreement that has been ratified, published, and entered into force for Bulgaria.

A crime also falls under Bulgarian jurisdiction **if it affects the interests of the Republic of Bulgaria or Bulgarian citizens**. Additionally, crimes committed abroad by foreign citizens may fall under Bulgarian jurisdiction if stipulated in an applicable international agreement. As a party to the European Convention on the Transfer of Proceedings in Criminal Matters, Bulgaria also exercises subsidiary jurisdiction in the cases provided for under Article 2 of the Convention. This jurisdiction is activated only upon a formal request for proceedings from another State Party to the Convention and when the criminal law of that State applies to the offense.

Bulgaria **complies with the requirements of Article 12 of the PIF Directive**, which specifies minimum limitation periods for criminal offenses involving VAT fraud. Under Bulgarian law, the limitation period for crimes against the tax system, including VAT fraud, **depends on the severity of the offense and the maximum penalty prescribed**.

The Bulgarian Criminal Code provides for varying penalties for different types of tax (VAT) fraud, with imprisonment ranging from 1 year up to 6, 8, or 10 years in the most serious cases [see

Articles 253¹³⁷ and following of the Criminal Code]. These varying penalties determine the corresponding limitation periods¹³⁸.

Croatia

In Croatia, to fight against VAT fraud, it is possible to **use several investigative tools and measures**. Some of the key tools and measures include:

- **Cooperation with the EPPO and Europol:** Croatia is cooperating with the European Public Prosecutor's Office (EPPO) and Europol in the fight against complex VAT fraud, including

¹³⁷ Article 253 C.C.:

(Amended, SG No. 28/1982, repealed, SG No. 10/1993, new, SG No. 62/1997)(1) (Amended, SG No. 85/1998, SG No. 26/2004, supplemented, SG No. 75/2006)

The one who concludes a financial operation or property transaction or conceals the origin, location, movement or the actual rights in the property, which is known or assumed to be acquired through crime or another act that is dangerous for the public, shall be punished for money laundering by imprisonment from one to six years and a fine from BGN three thousand to five thousand.

(2) (New, SG No. 26/2004, supplemented, SG No. 75/2006) The punishment under paragraph 1 shall also be imposed on the one who acquires, receives, holds, uses, transforms or assists, in any way whatsoever, the transformation of property, which is known or assumed, as of its receipt, to have been acquired through crime or another act that is dangerous for the public.

(3) (Renumbered from Paragraph 2, supplemented, SG No. 26/2004) The punishment shall be imprisonment for one to eight years and a fine from BGN five thousand to twenty thousand, if the act under paras 1 and 2 has been committed:

1. (amended, SG No. 26/2004) by two or more individuals, who have reached preliminary agreement, or by an individual who acts on the orders of or executes a decision of an organised criminal groups;

2. two or more times.

3. by an official within the sphere of his office.

4. (new, SG No. 26/2004) through opening or maintaining an account with a financial institution, under a false name or the name of an individual who has given consent to this effect.

(4) (New, SG No. 21/2000, renumbered from Paragraph 3, supplemented, SG No. 26/2004, amended, SG No. 75/2006)

The punishment shall be deprivation of liberty from three to twelve years and a fine from BGN 20,000 to BGN 200,000 where the act under Paragraphs (1) and (2) has been committed by the use of funds or property

which the perpetrator knew or supposed to have been acquired through a serious crime of intent.

(5) (New, SG No. 85/1998, renumbered from Paragraph 3, SG No. 21/2000, renumbered from Paragraph 4, amended, SG No. 26/2004, SG No. 75/2006) Where the funds or property are in extremely large amounts and the case is extremely grave, the punishment shall be imprisonment for five to fifteen years and a fine from BGN 10,000 to BGN 30,000, and the court shall suspend the rights of the guilty person under Items 6 and 7 of Article 37 (1).

(6) (New, SG No. 85/1998, renumbered from Paragraph 4, SG No. 21/2000, renumbered from Paragraph 5, amended, SG No. 26/2004) The object of crime or the property into which it has been transformed shall be forfeited to the benefit of the state, and where absent or alienated, its equivalent shall be awarded.

(7) (New, SG No. 26/2004) Provisions of paras 1 through 6 shall also apply where the crime through which property has been acquired falls outside the criminal jurisdiction of the Republic of Bulgaria

¹³⁸ Article 80 C.C.:

(1) Criminal prosecution shall be excluded by prescription where it has not been instigated in the course of: [...]

3. 10 years with respect to acts punishable by imprisonment for more than 3 years.

4. 5 years in respect of acts punishable by imprisonment for more than 1 year, and

5. 3 years in respect of all remaining cases.

[...]

carousel fraud. These institutions enable the rapid exchange of information and the coordination of transnational investigations.

- **Eurojust:** Eurojust provides support in judicial cooperation between EU Member States, allowing for more effective investigative measures and coordination between different national authorities. Through Eurojust, Croatia benefits from enhanced coordination and the implementation of effective investigative measures such as Joint Investigation Teams (JITs) and European Investigation Orders, which enable seamless collaboration among national authorities.
- **International cooperation:** Croatia leverages international mechanisms like the European Arrest Warrant and the European Investigation Order to ensure close collaboration with other EU Member States in tackling VAT fraud. These tools enable efficient cross-border investigations and prosecution of offenders.
- **Access to Tax Administration Data:** the Croatian Tax Administration has access to extensive databases containing financial transaction records, bank account details, and tax return information. This access facilitates the identification of suspicious activities and connected entities. Additionally, Croatia benefits from data shared by other EU Member States and third countries through bilateral treaties and international agreements, further enhancing its ability to combat fraud.

According to the expert, the investigative tools and measures used by Croatian law enforcement authorities can be effectively employed in investigating cyber VAT fraud. These tools include:

- **Collaboration with Europol and EPPO:** Croatian authorities work closely with Europol and the European Public Prosecutor's Office (EPPO) to combat complex VAT fraud schemes, including those involving cyber elements. This collaboration facilitates the exchange of intelligence and coordinated international operations.
- **Special investigative measures:** the use of special investigative measures such as wiretapping, surveillance, and the monitoring of financial transactions is crucial in detecting and proving cyber VAT fraud. These measures allow authorities to gather evidence on electronic communications and financial flows that are often involved in cyber-related fraud.
- **Advanced data analysis:** authorities utilize sophisticated data analysis tools to track and analyze large volumes of electronic data. This includes tracing digital footprints and analyzing patterns in financial transactions that indicate fraudulent activities.
- **Access to international databases:** through international cooperation, Croatian authorities have access to various databases and can cross-reference information with other EU member states. This helps in identifying and tracking cross-border fraud networks.
- **Cyber forensics:** cyber forensics involves the collection, preservation, analysis, and presentation of digital evidence. This is essential in investigating cyber VAT fraud, where digital evidence plays a key role.
- **Electronic data requests:** Croatian authorities can issue electronic data requests to service providers to obtain records of electronic communications and transactions that are relevant to the investigation.
- **Public-private partnerships:** collaborations with private sector entities such as banks and internet service providers are crucial. These partnerships enable quicker detection and

response to suspicious activities related to cyber VAT fraud. These investigative tools and measures are designed to be flexible and comprehensive, allowing Croatian law enforcement to effectively tackle both traditional and cyber-related VAT fraud.

According to the national expert, Croatia could strengthen its fight against VAT fraud by introducing several key measures aimed at improving the detection, investigation, and prosecution of such cases.

These **recommendations** include:

- **Enhanced data sharing and integration:** establishing a centralized database that consolidates information from tax authorities, customs, financial institutions, and law enforcement agencies would significantly enhance real-time data sharing and analysis. Such integration would improve collaboration among agencies and enable faster identification of fraudulent activities.
- **Implementation of advanced data analytics and AI tools:** leveraging data analytics and artificial intelligence (AI) tools can help detect anomalies and suspicious patterns across large datasets. These technologies would enable authorities to proactively identify potential fraud schemes and act swiftly to prevent losses.
- **Amendments to national legislation:** strengthening national laws by introducing stricter penalties for VAT fraud and related offenses could serve as a powerful deterrent. Harsher sanctions would signal a zero-tolerance approach and discourage individuals or entities from engaging in fraudulent practices.
- **Specialized training** for cyber security experts and investigators.
- **Promotion of advanced technology in tax reporting:** mandating the use of modern technology for tax reporting and compliance could significantly reduce opportunities for VAT fraud. Examples of such measures include:
 - **real-time fiscalization of B2B invoices:** ensuring that all business-to-business transactions are recorded and reported in real-time to tax authorities, minimizing the risk of unreported transactions;
 - **automated creation of tax records:** introducing systems for the automated generation of the Book of Sales and Book of Purchases for all taxpayers would enhance transparency and simplify compliance monitoring.

By adopting these measures, Croatia could improve its overall effectiveness in combating VAT fraud, ensuring stronger prevention, faster detection, and more successful prosecution of offenders.

Regarding **jurisdiction**, Croatia adheres to both the **principle of territoriality** and the **principle of personality**, which also extends to legal persons. This ensures that Croatian courts have jurisdiction over offenses committed within the territory, as well as offenses committed abroad by Croatian citizens or legal entities, provided such jurisdiction is established under national or international law. Criminal proceedings will be initiated only if the perpetrator is located on the territory of the Republic of Croatia.

Croatia is fully **compliant with Article 12 of the PIF Directive**. Like many other EU Member States (Austria, Belgium, Cyprus, Czech Republic, Hungary, Ireland, Poland, Romania, Sweden, and The Netherlands), Croatia has adopted legislation that ensures penalties for VAT fraud can be enforced

for at least five years from the date of the final conviction. Specifically, Croatian legislation provides for this enforcement period in two key scenarios:

- **when the penalty imposed is more than one year of imprisonment.**
- **when the penalty relates to a criminal offense punishable by a maximum sanction of at least four years of imprisonment.**

Cyprus

The national expert identified several tools and key elements that Cyprus can leverage in the fight against VAT fraud:

- Department Investigations Economic;
- Fraud Department of the Police;
- Local FIU (MOKAS - Monetary Unit and Financial Crimes Unit). It works closely with other domestic agencies, as well as international organizations like **Europol** and **Eurojust**, to tackle complex financial crimes that have cross-border implications;
- General Attorney.

When talking about cyber VAT fraud, it should be noted that Cyprus is the only European country to have specific substantive legislation for it. At the same time, a **dedicated Unit has also been established**, the Digital Fraud Investigation Unit from the Police.

Regarding the suggestions to improve the fight against VAT fraud and cyber VAT fraud, the national expert believes it is necessary to **invest in**:

- investigator training;
- enhanced collaboration with EU colleagues.

During the discussion, the expert emphasized the **upcoming mandate for e-invoicing in the EU** (2030 for B2B, 2027 for B2G) and highlighted the **potential of AI for detecting fraud**. The expert proposed that the EU develop unified digital tools to prevent fragmentation of national efforts; while AI could significantly streamline the detection process, open-source tools might pose security risks unless they are developed internally by the EU.

When analyzing the issue of **jurisdiction**, Cyprus adheres to the **principle of personality**, which includes nationality, habitual residence, Cypriot public officials, and also Cypriot legal entities. For proceedings to be initiated in the case of a Cypriot citizen's liability, it is essential that the prosecution can only be initiated after the victim files a report in the jurisdiction where the criminal offense occurred.

Regarding the **statute of limitations**, Cyprus is one of the few cases of **non-compliance with the Directive**, as it does not provide for minimum 5 years or even 3 years. It should be noted, however, that despite this, according to the EU VAT Gap report by the European Commission, Cyprus is the European country with the smallest VAT gap in 2022, standing at -0.7%¹³⁹.

¹³⁹ European Commission: Directorate-General for Taxation and Customs Union, Poniatowski, G., Bonch-Osmolovskiy, M., Śmietanka, A. and Pechcińska, A., "VAT gap in the EU – Report 2022", Publications Office of the European Union, 2022, retrieved from <https://data.europa.eu/doi/10.2778/109823>.

Czech Republic

With reference to the **tools for fighting VAT fraud**, starting from the **administrative control**, the national expert explained that the **controls' procedure for cross-border transactions** in the Czech Republic, as in other EU Member States, is the common EU system VIES.

Each VAT payer is required to submit a monthly VAT Control Statement, which details B2B transactions, including the VAT identification number of the business partner, the value of the supply, the date of supply, and the invoice number. The analytical software used by the financial administration identifies discrepancies between reported transactions, enabling tax authorities to uncover carousel fraud or situations where a VAT payer claims input VAT that has not been remitted by their supplier. The **ADIS software** system is employed by the financial administration to detect long-term discrepancies in the VAT liabilities reported by VAT payers.

If discrepancies are identified, VAT payers are questioned to understand why their reported VAT deviates for a particular taxable period, and whether VAT fraud was involved.

One investigative approach used by tax administrators is **local investigation**. Additionally, there is a procedure known as the “**doubt procedure**”, which is a fast and flexible method relying on reciprocal communication between the tax administrator and the taxpayer.

In 2022, the primary reasons for applying the doubt procedure were the unreliability of tax returns as assessed by the ADIS information system and the need to investigate VAT chain fraud. Out of nearly 10,000 doubt procedures initiated, more than 60% focused on VAT control, leading to a reduction in excessive VAT deductions of CZK 393 million [EUR 16.5 million] and an increase in tax liabilities by CZK 522 million approximately [EUR 21,924].

Tax audits are another common tool for investigating VAT fraud. In 2022, tax audits resulted in an additional VAT assessment totaling CZK 4,877 million [EUR 201,030,503]. The main reasons for initiating VAT audits included investigations into entities involved in VAT chain fraud. Frequent audit findings also involved unauthorized claims for tax deductions (violations of Section 72 of the VAT Act), failure to declare taxable transactions, verification of advance payments, and the correctness of tax rates. Data on VAT assessments from the doubt procedures and tax audits is drawn from the Annual Report on the Activities of the Financial Administration for 2022¹⁴⁰.

Regarding **criminal investigations**, it is important to highlight the **lack of tax or financial experts** within the police force.

The expert highlighted that in many criminal proceedings, the same administrative data are used, even though the focus and objectives of these two types of proceedings are completely different. Tax proceedings are based on evidence provided by the taxpayer, and if the taxpayer fails to provide such evidence, the tax administration can close the case to their disadvantage. However, this finding typically does not indicate the commission of a criminal offense. Criminal proceedings, on the other hand, rely on evidence presented by the police or prosecution, which must prove that a criminal offense has been committed. To address this, the police have established a **specialized national unit for investigating high-level criminal offenses related to tax matters**.

On a different note, there are **currently no specific tools in place for investigating cyber VAT fraud**. However, existing investigative tools can still be utilized.

¹⁴⁰www.financnisprava.cz/assets/cs/prilohy/fs-financni-sprava-cr/Vyrocní_zpráva_o_cinnosti_FS_CR_za_rok_2022.pdf.

Additionally, a **new regulation**, effective from January 1, 2024, **requires payment service providers to report specified cross-border money transfers**. This provision has been implemented in line with EU Directive 2020/284 (as regards introducing certain requirements for payment service providers).

Finally, the expert suggested that **banks reporting payment data from e-commerce transactions could play a significant role in combating cyber VAT fraud**. However, he raised concerns about whether this data is being processed and analyzed appropriately to effectively identify and address fraudulent activities.

As regards the **jurisdiction**, the Czech Republic applies both the **principle of territoriality** and the **principle of personality**, which also extends to legal persons, without conditions to start the criminal proceeding.

The Czech Republic is **compliant with Article 12 PIF Directive**. The relevant legal provision is Article 34 Criminal Code¹⁴¹. CR has adopted legislation that ensures penalties for VAT fraud can be

¹⁴¹ Article 34 C.C.:

Limitation period

- (1) Criminal liability for an offence is extinguished on the expiry of the limitation period, which is
- a) thirty years if the offence is an offence for which the Criminal Law permits the imposition of an exceptional penalty, and an offence committed in the preparation or approval of a privatization project under any other provision of law,
 - b) fifteen years, if the upper limit of the penalty is at least ten years of imprisonment,
 - c) ten years, if the upper limit of the penalty of imprisonment is at least five years,
 - d) five years, if the upper limit of the penalty of imprisonment is at least three years,
 - e) three years for other offences.
- (2) The limitation period shall begin to run for offences in which effect is a feature or in which effect is a feature of a qualifying offence from the time when such effect occurs; for other offences the limitation period shall begin to run from the end of the conduct. For a participant, the limitation period begins to run from the end of the act of the principal offender.
- (3) The statute of limitations does not include
- a) the period during which the offender could not be brought to trial because of a legal impediment,
 - b) the period during which the prosecution was suspended,
 - c) the period during which the victim of a crime of grievous bodily harm involving genital mutilation or sterilization (§ 145), unlawful termination of pregnancy without the consent of the pregnant woman (§ 159), trafficking in human beings (§ 168), introduction committed with intent to force another to marry (§ 172), extortion (§ 175) or oppression (§ 177) committed with intent to coerce another to marry or to tolerate an act tending to cause grievous bodily harm consisting of genital mutilation or any of the offences listed in Chapter Three of the Special Part of this Act on sexual offences against human dignity and/or the offence of enticement to sexual intercourse (§ 202) was under the age of eighteen,
 - d) probationary period of a conditional discontinuance of prosecution or a conditional deferral of the filing of a petition for punishment,
 - e) the period during which the offender could not be prosecuted in the Czech Republic, if the offence is an offence the criminality of which is assessed under the law of the Czech Republic on the basis of § 8(1),
 - f) the period from the making of the detention order until it is revoked or expires for any other reason,
 - g) the period during which certain acts of criminal proceedings have been temporarily dispensed with under the International Judicial Cooperation in Criminal Matters Act,
 - h) the period during which a criminal prosecution has been temporarily suspended.
- (4) The limitation period is interrupted
- a) the initiation of a criminal prosecution for the offence for which the limitation period is in question, as well as the subsequent taking into custody, the issuing of an arrest warrant, the lodging of a request for the arrest of a person from a foreign State, the issuing of a European Arrest Warrant, the the filing of an indictment, an application for the approval of a plea agreement, an application for punishment, the pronouncement of a conviction for that offence or the service of a warrant for that offence on the accused, or
 - b) if, within the limitation period, the offender has committed a new offence for which the Penal Law provides a penalty equal to or more severe.
- (5) The interruption of the limitation period starts a new limitation period.

enforced for at least five years from the date of the final conviction when the penalty is more than 1 year and for a criminal offense that is punishable by a maximum sanction of at least four years of imprisonment.

Denmark

In Denmark, the VAT compliance gap was estimated in 2022 at €3,360 million or 8.6% of the VAT total tax liability (VTTL), an increase of 4.1 percentage points compared to 2021.

Denmark estimates that fiscal and VAT fraud generate the largest proceeds of crime in its country¹⁴².

The national expert explained that in Denmark, the tax authority has broad access to any company at any time, as outlined in Article 74 of the Danish VAT Code. **In 2024, Denmark introduced several amendments to the Danish VAT Act to strengthen its efforts against tax fraud.** Key changes include a notification system designed to alert taxable persons who have purchased goods with unpaid VAT. Additionally, taxable persons are now required to declare VAT-exempt output transactions and report their input VAT ratio in an annual declaration.

In Denmark, the Money Laundering Secretariat has extensive **access to financial intelligence** and other information. These data can be used also against VAT fraud.

At the same time, a robust **digital reporting system**, which allows tax authorities to monitor and analyze VAT transactions, was implemented.

Danish authorities have organized much of their work related to financial crime in **specialized task forces**, which collaborate closely with the Financial Intelligence Unit: for new types of VAT fraud, for instance, a task force was settled with participants from the customs and tax authorities and the Public Prosecutor for Serious Economic Crime.

Although Denmark does not have specific tools for combating EU cyber VAT fraud, the expert emphasized that **digital reporting** and a **more expedited process** would be highly beneficial in addressing these issues.

Regarding Article 12 of the PIF Directive, Denmark is compliant and applies both the **principle of territoriality** and the **principle of personality**, which also extends to legal persons, without conditions to start the criminal proceeding.

The **limitation period** is at least 5 years for the criminal offense of VAT fraud, as provided for in Article 12 of the PIF Directive.

Estonia

Although no responses were collected from the questionnaire, information about the investigative tools used in Estonia can be reported thanks to the research conducted by the CSSC.

¹⁴² Faft, "Anti-money laundering and counter-terrorist financing measures, Denmark Mutual Evaluation Report 2017" retrieved from: <https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/MER-Denmark-2017.pdf>.

Estonia ranked **9th among the EU Member States**, with a VAT compliance gap estimated at €152 million or 4.4% of the VAT total tax liability (VTTL) in 2022, and an increase of 2.9 percentage points compared to 2021¹⁴³.

In Estonia, the **tax administration conducts investigations, directed by a prosecutor/examining judge**.

Estonian Tax and Customs Board uses **big data and data analytics technology** for **fraud detection and evaluation purposes**. This system allows to identifying risk coefficient for each case with the overall objective of increasing tax compliance and preventing frauds. For this purpose, EMTA analyses a large amount of structured data coming from government sources, mainly such as business registers and tax declarations¹⁴⁴.

It is possible to use also the “**traditional**” **investigative tools**, for instance seizures and confiscation, inspections, and audit.

The **jurisdictional criterion** is based mainly on the **principle of personality**.

Estonia is **compliant with Article 12 of the Directive**: the limitation period is 6 years for VAT fraud and 5 for tax evasion. As a general rule, the statute of limitations is three years.

Finland

Finland is **highly proactive in both preventing and combating VAT fraud**, achieving one of the lowest VAT gaps in Europe.

The country **works closely with Europol, Eurojust, and other relevant authorities to strengthen its efforts**. There is **extensive information-sharing** among these authorities, allowing for **cross-checks** and the consolidation of data from various sources. Finland utilizes a range of traditional investigative tools, including **inspections, seizures, and audits**. Moreover, Finland has established a comprehensive legal framework for asset recovery, including effective mechanisms to facilitate asset confiscation decisions.

Regarding **jurisdiction**, Finland applies both the **principles of territoriality and personality**.

For the latter, there are **no specific conditions required to establish jurisdiction**.

Finland **complies with Article 12** of the PIF Directive, ensuring a minimum limitation period of **5 years**. A penalty for VAT fraud can be enforced for at least five years from the date of the final conviction if the penalty involves more than one year of imprisonment, or if the offense carries a maximum penalty of at least four years of imprisonment.

France

The French national expert highlighted several key investigative tools and measures that are **effectively employed to combat VAT fraud**:

- customs police investigation;

¹⁴³ See footnote no 125.

¹⁴⁴ European Commission, “Study on “Data Analytics for Member States and Citizens”, 2020, retrieved from <https://interoperable-europe.ec.europa.eu/collection/study-data-analytics-member-states-and-citizens>.

- random treasury tax audits;
- data analysis and technology (Tracfin);
- international cooperation (Europol alerts);
- inquiries and interrogations;
- surveillance and monitoring and document analysis.

These instruments can also be applied to combat cyber VAT fraud. Given the unique aspects of cyber VAT fraud, it is crucial to incorporate additional specialized tools and techniques to effectively address these challenges:

- electronic transaction monitoring;
- digital data analysis;
- digital forensic analysis;
- online activity streaming;
- technological business cooperation;
- metadata analysis.

According to the national expert, the French Criminal Procedure **could be improved by adapting the directives, as well as, by updating the legislation, by creating specific articles in the Criminal Code that would deal more specifically with crimes against the Public Administration.** Therefore, it is necessary to clearly define the crime, and its penalties and for these to be more effective, thus avoiding an increase in the recurrence of crimes linked to any type of VAT fraud or cyber VAT fraud.

In France, the **jurisdictional criterion** primarily follows the principle of **territoriality**. According to Article 11, paragraph 4 of the PIF Directive, **when the principle of personality is applied, certain conditions are excluded.** Specifically, in France, the prosecution **can only be initiated if there has been a report from the state where the criminal offense was committed.**

France does **not fully comply with Article 12 of the PIF Directive** regarding the limitation period, as its statute of limitations is **shorter than the required 5 years, and in some cases, even shorter than 3 years.**

Germany

To ensure that activities comply with their value-added tax (VAT) obligations, the tax office can **conduct a surprise VAT inspection.**

In addition, other “traditional” investigative tools are applicable:

- **inspections and seizures;**
- **fraud risk assessments;**
- **significant international cooperation.**

In Germany, the **Federal Cartel Office can not wiretap or conduct electronic surveillance.**

Telecommunications surveillance may only be ordered by a court upon the public prosecution office's application, and only in cases involving a bid-rigging offense under Article 298 of the Criminal Code¹⁴⁵.

Germany includes in its **jurisdiction** every case of VAT evasion, regardless of where the offense was committed and the identity of the perpetrator, according to Section 370 (6) AO ¹⁴⁶. Germany follows both the principle of territoriality and personality.

¹⁴⁵ Section 298 C.C.

Collusive tendering

(1) Whoever, in connection with an invitation to tender relating to goods or services, makes an offer based on an unlawful agreement whose purpose is to cause the organiser to accept a specific offer incurs a penalty of imprisonment for a term not exceeding five years or a fine.

(2) The award of a contract by direct agreement following a prior call for competition is equivalent to an invitation to tender within the meaning of subsection (1).

(3) Whoever voluntarily prevents the organiser from accepting the offer or from providing a service does not incur the penalty specified in subsection (1), also in conjunction with subsection (2). If the offer is not accepted or the organiser's service is not rendered without any action on the offender's part, no penalty is incurred if the offender makes voluntary and earnest efforts to prevent the offer being accepted or the service being rendered.

¹⁴⁶ Abgabenordnung (AO) § 370

Tax Evasion

(1) Whoever

1. provides incorrect or incomplete information to the tax authorities or other authorities about tax-relevant facts,
2. intentionally omits to inform the tax authorities about tax-relevant facts, or
3. intentionally fails to use tax stamps or tax stamps improperly and thereby reduces taxes or obtains unjustified tax advantages for themselves or others, shall be punished by imprisonment of up to five years or a fine.

(2) Attempted offenses are punishable.

(3) In particularly serious cases, the punishment is imprisonment for six months to ten years. A particularly serious case is typically present if the offender

1. reduces taxes or obtains unjustified tax advantages to a large extent,
2. abuses their powers or position as a public official or European public official (as per § 11 paragraph 1 no. 2a of the Penal Code),
3. exploits the assistance of a public official or European public official (§ 11 paragraph 1 no. 2a of the Penal Code) who abuses their powers or position,
4. continues to reduce taxes or obtain unjustified tax advantages using forged or falsified documents,
5. as a member of a gang that has formed to continuously commit offenses under paragraph 1, reduces sales or consumption taxes or obtains unjustified sales or consumption tax advantages, or
6. uses a third-country company as defined in § 138 paragraph 3, which they alone or together with related persons, as per § 1 paragraph 2 of the Foreign Tax Act, can exert direct or indirect control over, to conceal tax-relevant facts and thus continuously reduce taxes or obtain unjustified tax advantages.

(4) Taxes are considered reduced when they are not, not fully, or not timely assessed; this also applies when the tax is provisionally or subject to review. Tax advantages include tax refunds; unjustified tax advantages are those that are granted or left unjustified. The conditions of sentences 1 and 2 are also met if the tax related to the offense could have been reduced or the tax advantage could have been claimed for other reasons.

(5) The offense can also be committed concerning goods whose import, export, or transit is prohibited.

(6) Paragraphs 1 through 5 also apply to cases involving import or export duties administered by another EU member state or duties that belong to a member state of the European Free Trade Association or an associated state. The same applies to cases involving VAT or harmonized excise duties under Article 1 paragraph 1 of Council Directive 2008/118/EC of December 16, 2008, on the general system of excise duties and the repeal of Directive 92/12/EEC, administered by another EU member state.

(7) Paragraphs 1 through 6 apply regardless of the law of the place where the offense occurred, also to offenses committed outside the scope of this law.

With regard to the **limitation period**, Germany is **compliant** with Article 12 of the PIF Directive, because the provisions are:

- 5 years in case of involuntary tax evasion;
- 10 years in case of voluntary tax evasion.

In Germany, indeed, VAT fraud is prosecuted **for both intent and negligence**.

Greece

According to the national expert, in the fight against VAT fraud, the **Financial Police Directorate** plays a pivotal role. As part of its collaboration with European organizations, executives from the **Financial Police Directorate of the Hellenic Police** have been appointed as experts in various **EUROPOL Analysis Projects**¹⁴⁷.

The **Financial Police Directorate** has adopted an **intelligence-led policing (ILP) approach**, focusing on actions aimed at prosecuting crimes that directly impact state revenue. These include offenses arising from **tax and customs legislation** as well as **violations of insurance laws**.

To fulfill its mission, the Directorate's core tasks involve the **collection, analysis, and processing of information**, both for **operational use** and to **derive strategic forensic insights**. To support this, an **information database** is maintained.

A key component in achieving these objectives is the **Information System (IS)**, developed by specialized personnel from the **Information Management and Strategy Departments**. This system comprises the **Information Management System (IMS)** software and the necessary **technological infrastructure**. The collected data undergoes **evaluation, parameterization, and analysis** at both **strategic and operational levels**.

Additionally, the **Financial Police Directorate** has **direct access to information systems and electronic applications** of other agencies, enabling authorized personnel to enhance investigative efforts.

The Directorate conducts **systematic and targeted audits** based on a **comprehensive risk analysis process**. This involves assessing the current landscape and categorizing collected information using **measurable quantitative indicators**. Open-source research, including Internet and publication analysis, further contributes to identifying trends and threats associated with financial crimes.

Specially trained **business analysts** play a critical role in processing incoming intelligence using the **4x4 evaluation system**. This ensures that data is effectively parameterized for integration into **structured forensic analysis databases**, including **MS Access** and **IBM i2**.

The same tools are utilized for investigating **cyber VAT fraud**. A **special control procedure** ensures **unhindered access** to all types of **documents, records, and other relevant materials**, facilitating the work of audit bodies and authorities responsible for detecting and investigating **tax evasion and VAT fraud**.

Specifically, under **Article 15 of Law 4144/2013**, as amended and currently in force, it is stipulated that **documents, records, certificates, licenses, and any legally mandated information**—which must

¹⁴⁷ (as for instance, AWF S.O.C./A.P. MTIC, AWF S.O.C./A.P. SUSTRANS and AWF S.O.C./A.P. SMOKE).

be presented to the **audit bodies of Social Security Funds (IKA-ETAM and SEPE)**—must also be made available to the **Financial Police Directorate of the Hellenic Police** and the **auditors of the Financial Crime Prosecution Corps (S.D.O.E.) of the Ministry of Finance**. This requirement applies within the framework of audits conducted by **Article 14 of the same law**.

Following the completion of audits under **Article 14**, the competent **audit bodies of the Financial Police Directorate** and the **Financial Crime Prosecution Corps (S.D.O.E.)** are required to **prepare and submit a detailed report** documenting their findings.

The **introduction of obligations for payment service providers** is also strategic in to fight against VAT fraud and cyber VAT fraud for the national expert.

Greece mainly applies the **principle of territoriality** in matters of **jurisdiction**.

According to Article 26, Paragraph 2 of Law 4689/2020, Greek criminal courts have jurisdiction over offenses listed in Articles 23 and 24 of the same law, as well as offenses under:

- articles 159, 159A, 235, 236, 237, 237B, 375, 386, 386A, 386B, and 390 of the Criminal Code.
- article 155 et seq. of Law 2960/2001 (A' 265).
- article 39 of Law 4557/2018 (A' 139).

When these offenses are directed against the financial interests of the European Union or are linked to their infringement, jurisdiction is established even when these offenses are committed abroad by a Greek citizen, regardless of whether the act is punishable under the laws of the country where it was committed. Additionally, Greek jurisdiction applies even if the **conditions of Paragraph 3, Article 6 of the Civil Code** are not met.

As a result, the **exercise of Greek jurisdiction is not contingent** on:

- a **complaint by the victim** in the country where the crime occurred; or
- a **formal denunciation by the state** where the crime was committed.

Furthermore, **Article 5, Paragraph 1 of the Greek Criminal Code** states that **Greek criminal laws apply to all acts committed within Greek territory**, even when committed by **foreign nationals**. Greek law also applies to **acts of participation in a crime committed within Greece**, even if the **main offense**—for which Greek criminal courts may lack jurisdiction—is **also punishable under Greek law**.

Greece is **compliant with Article 12 of the PIF Directive**, by providing a limitation period of more than 5 years. Article 111 par.2 of the Greek Penal Law (4619/2019) regarding the statute of limitation of crimes provides that *“Felony is time-barred after twenty years if the law provides for life imprisonment and after fifteen years in any other case, unless the law provides otherwise”*.

Hungary

According to the national expert, in Hungary, **only the courts have the authority to determine whether a crime has been committed**. Court proceedings are initiated when the **public prosecutor files charges** and the court is bound by the **charges outlined in the indictment**.

During the court procedure, the **principle of free assessment of evidence applies**, meaning the court independently evaluates the evidence presented. While courts in criminal proceedings are

not bound by decisions made in **civil, administrative, or other legal procedures**, they may consider **and use** evidence gathered by other authorities.

VAT fraud investigations rely heavily on **documentary evidence**, including:

- **fiscal records**: VAT returns, financial statements, general ledgers, invoices, and contracts.
- **public registry documents**: company register, land registry, and other official records.

In addition, **competent authorities** may conduct **on-site investigative actions**, such as:

- **search of premises.**
- **confiscation/seizure of relevant items.**
- **test purchases to verify fraudulent activity.**

Authorities may also employ **surveillance measures** (subject to authorization from a **public prosecutor or judge**) and **collect witness statements** to support the investigation.

In Hungary, **all standard investigative tools and measures** applicable to criminal investigations can also be used in cyber-VAT fraud cases. There are no specialized investigative measures exclusively for cyber-VAT fraud.

Regarding jurisdiction, Hungary applies **both the personality principle** (without conditions) and the **territoriality principle**. Notably, under the territoriality principle, Hungarian jurisdiction extends to criminal offenses committed on board a craft or aircraft bearing the **Hungarian flag**, regardless of where the vessel is located at the time of the offense.

Hungary is **compliant with Article 12 of the PIF Directive**, which specifies a **minimum limitation period of five years** for the criminal offense of VAT fraud. Similar to most of the respondents (including Austria, Belgium, Croatia, Cyprus, Czech Republic, Ireland, Poland, Romania, Sweden, and the Netherlands), Hungary specifies that penalties for VAT fraud can be enforced for at least five years from the date of the final conviction, whether the penalty involves more than one year of imprisonment or a sentence for a crime punishable by up to four years of imprisonment.

Ireland

Investigations and prosecutions of VAT fraud in Ireland involve **multiple enforcement authorities** within the criminal justice system. The key agencies include:

- **An Garda Síochána** (Ireland's national police service).
- **the Office of the Director of Public Prosecutions.**
- **the Office of the Revenue Commissioners.**

According to the national expert, within An Garda Síochána, the **Garda National Economic Crime Bureau (GNECB)** plays a leading role in tackling economic crime, including VAT fraud. In recent years, there has been a **growing emphasis on multi-agency investigations**, particularly in cases of suspected VAT fraud. Additionally, the newly established **Corporate Enforcement Authority** may become increasingly relevant in cases of company-based fraud.

Law enforcement authorities in Ireland primarily rely on **standard investigative measures**, including:

- **searches of property;**

- **data gathering;**
- **seizure of digital and physical records;**
- **production orders** served on financial institutions;
- **monitoring of financial transactions.**

The **Revenue Commissioners** employ a **data-driven approach** to identifying discrepancies and non-compliance. This involves analysing **taxpayer returns, third-party information, and other intelligence sources**. An increasingly valuable tool is the use of **Suspicious Transaction Reports (STRs)** submitted by financial institutions and designated bodies. In 2023, Revenue received **over 72,900 STRs**, reflecting a **73% increase from 2022**¹⁴⁸.

The national expert noted that a key limitation in Ireland's approach to VAT fraud enforcement is its **non-participation in the European Public Prosecutor's Office (EPPO)**. While Ireland has provisions for **cooperation with non-participating EU member states**, the **European Chief Prosecutor has formally noted** that Ireland has **consistently refused EPPO requests for judicial cooperation**¹⁴⁹. This lack of participation **restricts access to crucial evidence** in cross-border VAT fraud investigations. Ireland's stance on EPPO participation appears **unlikely to change** in the near future.

There is currently **no evidence of major differences with respect to investigative tools/measures in Ireland between cyber and non-cyber VAT fraud**. While there is an Irish enforcement body for cybercrimes (Garda National Cyber Crime Bureau), this body is concerned primarily with forensic evidence and investigations into ransomware, malware, and hacking.

According to the national expert, overall cyber VAT fraud does not seem to be among the priorities identified in Ireland's cybercrime strategies. This lack of cyber VAT fraud enforcement measures is regrettable, particularly given **Ireland's position as a jurisdiction of choice for various "Big Tech" multinational companies**, which hold vast amounts of valuable personal and communications data.

Finally, the expert discussed Ireland's **challenges with electronic data in criminal cases**, highlighting the need for comprehensive legislation on data holding, access, and judicial oversight in relation to digital evidence.

The expert highlighted also that Ireland has recently had the benefit of a **Review Group Report on structures and strategies to prevent, investigate, and penalise economic crime and corruption**. This expert Review Group identified various issues which the Department of Justice has already committed to addressing through the "Implementation Plan".

Structural/systemic recommendations of the Implementation Plan include:

- Ensuring adequate resources for the GNECB via long-term strategic planning.
- Joint training programs for investigators of economic crime and corruption.
- Optimising exchange of information/intelligence to allow for Joint Agency Task Force models.

¹⁴⁸ Office of the Revenue Commissioners, Annual Report 2023.

¹⁴⁹ Letter to the European Commission, 23 Nov 2021.

Further, according to the Criminal Assets Bureau¹⁵⁰, abuse of VAT schemes has become prevalent in the second-hand motor trade in Ireland. This industry has reportedly been infiltrated by organised crime groups along the Northern Ireland border.

Regarding jurisdiction, both the territoriality and personality principles apply, in full accordance with all provisions of Article 11 of the PIF Directive.

In relation to the **limitation period**, it should be noted that there was no specified limitation period added to the Criminal Justice (Theft and Fraud Offences) Act 2001 as amended during the transposition of the PIF Directive.

Similar to most of the respondents (including Austria, Belgium, Croatia, Cyprus, Czech Republic, Hungary, Poland, Romania, Sweden, and the Netherlands), Ireland specifies that penalties for VAT fraud can be enforced for at least five years from the date of the final conviction, whether the penalty involves more than one year of imprisonment or a sentence for a crime punishable by up to four years of imprisonment.

Italy

In Italy, several investigative tools can be used to combat VAT fraud. These tools come from both traditional financial investigations and more advanced methods, including those used for cybercrime. Some of the key instruments include:

1. **Financial and Accounting Audits** – Authorities, such as the Guardia di Finanza, conduct in-depth audits of company financial records to identify irregularities in VAT payments.
2. **Cross-Border Cooperation and Data Exchange** – Italy collaborates with other EU member states through mechanisms like EUROFISC, a network that facilitates real-time information sharing on VAT fraud.
3. **Electronic Invoicing and Digital Reporting** – The mandatory use of electronic invoicing and the "Sistema di Interscambio" (SdI) help authorities monitor transactions and detect anomalies.
4. **Bank and Financial Transaction Analysis** – Investigators can access banking records to trace suspicious movements of money related to VAT fraud schemes.
5. **Means of searching for evidence, i.e.: inspections, searches** (both personal and local), **seizures** (assets, but also computer data).
6. **Wiretapping and Surveillance** – In cases of serious fraud, authorities may use wiretapping and covert surveillance to gather evidence against criminal networks.
7. **Artificial Intelligence and Big Data Analytics** – Advanced data analysis tools are increasingly used to detect patterns indicative of fraudulent behavior, such as carousel fraud.
8. **Cybercrime Investigation Tools** – When VAT fraud involves digital platforms or cryptocurrencies, authorities employ cyber forensic techniques similar to those used against cybercrime.

¹⁵⁰ Criminal Assets Bureau, Annual Report 2022.

These tools, used in combination, help Italian authorities detect, investigate, and prosecute VAT fraud effectively.

There are **no other specific investigative tools to combat VAT cyber fraud**, but it is possible to use the means of proof and the investigative tools typical of traditional VAT fraud, as well as the instruments dedicated to cybercrime in general, in the case of cyber VAT fraud. This openness, however, is not sufficient. The assessment framework remains the most complex and multifaceted one, compared to the substantive part.

Italian legislation has introduced electronic invoicing since 2019: the transmission of this data, visible to the financial administration, makes it easier for investigators to identify carousel fraud.

During the discussion on the focus groups, it was proposed to expand investigations beyond financial transactions to include communications and system monitoring (e.g. **lawful hacking**), even if it is always difficult to balance this need with data protection and privacy rights.

The Italian stakeholder suggested that tools such as **real-time monitoring of financial transactions and the identification of IP addresses are needed to prosecute fraudsters more effectively**. At the same time, it would be very useful for a **single European business register** and the **use of biometric authentication** for financial services to better identify individuals involved in fraud.

All the proposals consider the other side of the technology, and the potential ethical issues associated with using intrusive technologies like AI and data mining in investigations.

Regarding **jurisdiction**, in Italy, it is applied both the **criterion of territoriality and personality**, and in case of the participation of criminal organisations operating totally or partially in Italy.

Article 11, paragraph 4 of the PIF Directive provides that, in cases where the personality principle applies, certain conditions are excluded. In Italy, no conditions are excluded.

In relation to the **limitation period**, Italy is compliant with the PIF Directive: it is foreseen a period of at least 6 years for felonies¹⁵¹ (as it is VAT fraud).

Latvia

The **Latvian Tax and Customs Police** has access to a **comprehensive range of investigative tools and methods** for combating **VAT fraud**, with no notable restrictions. This includes the **full spectrum of investigative techniques**, particularly given that **VAT fraud cases** frequently qualify as **serious crimes**.

The **importance of operational investigative work cannot be overstated**, as it facilitates **real-time data collection and intelligence gathering**. Analytical efforts, especially in cooperation with the **State Revenue Service (SRS)**, play a **crucial role** in detecting and dismantling fraud schemes.

¹⁵¹ Art. 157 Italian Criminal Code:

The statute of limitations extinguishes the crime after the expiry of the time corresponding to the maximum statutory penalty established by law and in any case a period of no less than six years in the case of a crime and four years in the case of a contravention, even if punished only with a financial penalty.

This provision must be integrated with:

Art. 17 D. Lgs. 74/2000:

The course of the statute of limitations for the crimes envisaged by this decree is interrupted, in addition to the acts indicated in article 160 of the penal code, by the report of findings or by the act of ascertainment of the relevant violations. 1-bis. The statute of limitations for the crimes provided for in articles 2 to 10 of this decree are increased by one third.

According to the national expert, Latvia often functions as an **intermediary jurisdiction**, with the **primary beneficiaries of VAT fraud** located **outside the country**. Given the **significant economic impact** of large-scale VAT fraud, enhanced cross-border cooperation and intelligence-sharing remain essential.

Fraud affecting the **national budget** is addressed through a **robust reporting framework** for **suspicious transactions**, supported by financial institutions, the Financial Intelligence Unit (FIU), and law enforcement agencies (PPPs). This **comprehensive approach** has yielded results **exceeding the EU average**, as reflected in the **2022 VAT Gap Report** compiled by the **European Commission** and the **State Revenue Service (SRS)**.

The **existing investigative tools and measures** can be **effectively adapted to the digital environment**, provided there is a **continuous commitment** to advancing expertise and adopting **best practices** from across jurisdictions. The **digital landscape** presents **unique challenges**, requiring **ongoing innovation** in investigative techniques. **International collaboration** is crucial, with the **European Public Prosecutor's Office (EPPO)** playing a key role. It may be worth considering a **lowering of the prosecutorial threshold** within the **EPPO framework**, though this would necessitate **expanding its operational capacity**, including an **increase in personnel**.

In the opinion of the expert, to **enhance the effectiveness** of national criminal procedures in combating **VAT fraud**, it is essential to **streamline and harmonize** the **regulatory framework** at the **European Union level**. Establishing **consistent practices** across Member States and recognizing **tax administration risk assessments** as **admissible evidence** in criminal proceedings would be **significant steps forward**. Additionally, developing **efficient cooperation mechanisms**, both **domestically and internationally**, would further strengthen **investigative efforts**.

The **current lack of harmonization** in **procedural standards** and **evidentiary requirements** across the EU remains a **major obstacle** to the effective prosecution of **VAT fraud**. Addressing these issues through **legislative and procedural reforms** would **significantly improve enforcement outcomes** and enhance **cross-border cooperation**.

In Latvia, both the **territoriality principle** and **personality principle** are applicable. Article 11, paragraph 4 of the PIF Directive states that when the **personality principle** applies, certain **conditions are excluded** — a provision that Latvia **fully implements** without any additional requirements.

The **digital environment** presents **unique complexities** that remain inadequately addressed by existing **national criminal procedures**, particularly due to the **absence of established judicial precedents** in this domain. A key challenge is the **determination of jurisdiction**, especially when an alleged offender is subject to **investigation in multiple countries**, but prosecution is **confined to a single jurisdiction**. This **jurisdictional ambiguity** can significantly hinder effective enforcement efforts.

To address these challenges, it is imperative to:

- **develop new legal frameworks** that clearly define **jurisdictional authority** in digital cases.
- **establish international cooperation protocols** to streamline **cross-border investigations and prosecutions**.
- **enhance information-sharing mechanisms** among enforcement agencies to prevent jurisdictional conflicts.

According to the national expert, a **coordinated EU-wide approach** will be essential to ensure **efficient enforcement** and **strengthen the legal foundation** for tackling digital VAT fraud and other financial crimes.

About the **limitation period**, Latvia is compliant with Article 12 of the PIF Directive, providing a **duration of at least 5 years** [see Article 56 C.C.¹⁵²].

Lithuania

The **Code of Criminal Procedure of Lithuania** provides a comprehensive and **exhaustive list of admissible means of proof**, which include:

- **testimony** from the **suspect, accused, victim, or witness**.
- **expert reports** and **specialist conclusions**.
- **physical evidence**, such as **items and documents**.

During the **pre-trial investigation** of any criminal offense, including **cyber VAT fraud**, law enforcement authorities—such as **pre-trial investigators, prosecutors, pre-trial judges, and courts**—are empowered to conduct **procedural coercive measures** and **investigative actions** as outlined in the **Code of Criminal Procedure**.

These **measures and actions** include:

- **Coercive measures:**
 - provisional arrest;
 - committal of a suspect to a medical institution;
 - detention and bringing in of a person;
 - temporary removal from office;
 - temporary restriction of property rights.
- **Investigative actions:**
 - searches and seizures;
 - taking of samples for comparative analysis;
 - collection of photographic, video, fingerprint, and genetic dactyloscopy data;
 - covert surveillance and undercover investigations;
 - simulation of a criminal act;
 - interviews, confrontations, and identification parades;
 - on-site verification of testimonies, crime scene examinations, and forensic analyses.

¹⁵² Art. 56. Criminal Liability Limitation Period

(1) A person may not be held criminally liable if from the day when he or she committed the criminal offence, the following time period has elapsed:

[...]

3) five years after the day of committing a less serious crime.

4) ten years after the day of committing a serious crime.

This **broad range of tools** ensures that Lithuanian authorities have the necessary legal framework to **effectively investigate and prosecute VAT fraud**, particularly in the **digital sphere**, where complex forensic techniques and intelligence-gathering methods play a crucial role.

In the opinion of the majority of experts, currently **the procedural measures provided for by the Code of Criminal Procedure and Law on Criminal Intelligence** are sufficient for the investigation of criminal cases of VAT fraud.

With regard to **jurisdiction**, Lithuania applies both the **territoriality and personality principles**. Article 11, paragraph 4 of the **PIF Directive** states that when the **personality principle** applies, certain **conditions are excluded** – a provision that Lithuania **fully implements** with only an additional requirement [see Article 8 C.P.C.¹⁵³].

Lithuania is **compliant with Article 12 of the OIF Directive on the limitation period of at least 5 years** [see Article 95 C.P.C.¹⁵⁴ lit. C].

¹⁵³ Article 8 C.P.C.

Criminal Liability for the Crimes Committed Abroad

1. A person who has committed abroad the crimes [...] shall be held criminally liable only where the committed act is recognised as a crime and is punishable under the criminal code of the state of the place of commission of the crime and the Criminal Code of the Republic of Lithuania. Where a person who has committed a crime abroad is prosecuted in the Republic of Lithuania, but a different penalty is provided for this crime in each country, the person shall be subject to a penalty according to laws of the Republic of Lithuania, however it may not exceed the maximum penalty specified in criminal laws of the state of the place of commission of the crime.

[...]

¹⁵⁴ Article 95 of C.P.C.

Statute of Limitations of a Judgment of Conviction

1. A person who has committed a criminal act may not be subject to a judgment of conviction where:

1) the following period has lapsed:

- a) three years, in the event of commission of a misdemeanor;
- b) eight years, in the event of commission of a negligent or minor premeditated crime.
- c) twelve years, in the event of commission of a less serious premeditated crime.
- d) fifteen years, in the event of commission of a serious crime.
- e) twenty-five years, in the event of commission of a grave crime.
- f) thirty years, in the event of commission of a crime relating to a premeditated homicide.

2) within the period laid down in point 1 of paragraph 1 of this Article, the person did not hide from pre-trial investigation or a trial and did not commit a new criminal act.

2. The statute of limitations shall run from the commission of a criminal act until the passing of a judgment.

3. If a minor suffers from the criminal acts provided for in Chapters XVIII, XX, XXI, XXIII and XLIV of this Code, the statute of limitations may not run out before the person reaches the age of twenty-five years.

4. Where a person who has committed a criminal act hides from pre-trial investigation or a trial, the statute of limitations shall not run. The statute of limitations shall resume running from the day when the person is detained or when he appears before a pre-trial investigation officer, a prosecutor or a court. However, a judgment of conviction may not be passed where twenty-five years have lapsed since the commission of the criminal act by the person and thirty years have lapsed since the commission of a crime relating to a premeditated homicide, and the statute of limitations has not stopped running due to commission of a new crime.

5. Where a person who has committed a criminal act enjoys, under laws of the Republic of Lithuania or international legal norms, immunity from criminal liability and the competent authority does not allow his prosecution, the statute of limitations stops running. The statute of limitations shall resume running from the receipt of the competent authority's permission to prosecute the person who has committed the criminal act or after he loses immunity as referred to in this paragraph by other means.

6. In the course of hearing of a case before the court, the statute of limitations shall stop running for a period for which:

1) the court announces a break in the hearing before the court or postpones the hearing of the case due to the absence of the accused or his defense counsel.

Luxembourg

The fight against VAT fraud in Luxembourg relies on **several key actors**, particularly the **Anti-Fraud Unit** of the VAT authorities (Service Anti-Fraude).

The pivotal role of the Anti-Fraud Unit is further underscored by the **volume of assistance** requests within the framework of **administrative cooperation with EU countries**—an essential aspect of combating VAT fraud given its **transnational nature**. In 2023, the unit received 192 requests for assistance from other Member States, along with four spontaneous disclosures related to foreign taxpayers.

Conversely, the Anti-Fraud Unit actively sought cooperation from other Member States through 102 assistance requests and 16 spontaneous disclosures concerning cross-border transactions either originating from or destined for Luxembourg¹⁵⁵.

There are also other tools and measures already in place in the fight against VAT fraud. For example, as of today:

- **Early Warning System** (automated screening of the monthly, quarterly, and annual returns submitted by the taxpayers);
- **standard audits of the VAT authorities**;
- **exchange of information** with authorities of other MS.

Theoretically, these instruments **can also be utilized in the fight against cyber VAT fraud**. However, technological limitations pose a significant barrier.

2) the court announces a break in the hearing before the court pending an expert examination or a professional investigation assigned by the court or satisfaction of a request for legal assistance submitted to a foreign state.

3) the court announces a break in the hearing before the court and charges a prosecutor or a pre-trial investigation judge with taking the procedural actions provided for in the Code of Criminal Procedure of the Republic of Lithuania.

4) the court announces a break in the hearing before the court for the new defense counsel of the accused to familiarise with the case file.

7. In the cases provided for in paragraph 5 of this Article, a judgment of conviction cannot be passed where a period exceeding that provided for in paragraph 1 by five years has lapsed since the commencement of the statute of limitations.

8. Where a person commits a new premeditated criminal act before the expiry of the terms indicated in this Article, the statute of limitations shall stop running. In such a case, the statute of limitations in respect of the first criminal act shall start to run from the commission of a new crime or misdemeanor.

9. The following crimes provided for in this Code shall have no statute of limitations:

1) genocide (Article 99);

2) treatment of persons prohibited under international law (Article 100);

3) enforced disappearance (Article 100¹);

4) killing of the persons protected under international humanitarian law (Article 101);

5) deportation or transfer of civilians (Article 102);

6) causing bodily harm to, torture or other inhuman treatment of the persons protected under international humanitarian law or violation of protection of their property (Article 103);

7) forcible use of civilians or prisoners of war in the armed forces of the enemy (Article 105);

8) destruction of protected objects or plunder of national valuable properties (Article 106);

9) aggression (Article 110);

10) prohibited military attack (Article 111);

11) use of prohibited means of warfare (Article 112);

12) negligent performance of the commander's duties

¹⁵⁵ Ministère des Finances, Rapport d'activité, exercice 2023, Attributions de l'administration de l'enregistrement, des domaines et de la TVA, 2023.

Regarding **jurisdiction**, both **the territoriality and personality principles apply**. Article 11, paragraph 4 of the PIF Directive stipulates that when the personality principle is applied, certain conditions are excluded. For Luxembourg, there are no exclusions.

Luxembourg **complies with Article 12 of the PIF Directive**, establishing a limitation period of **10 years, or 5 years for offenses punishable by correction** [See Articles 637¹⁵⁶ and 638¹⁵⁷, Code of Criminal Procedure, L. 2009/6].

Malta

In Malta, authorities employ a range of investigative tools to combat VAT fraud, integrating both traditional methods and advanced technological solutions. Key instruments include:

1. **Data Analytics and Artificial Intelligence (AI):** The Malta Tax and Customs Administration (MTCA) utilizes advanced data analytics and AI to automatically detect compliance discrepancies and filing errors. By analyzing extensive datasets, these technologies identify suspicious transactions and potential violations of tax regulations, enhancing the detection of irregular trading patterns associated with VAT fraud.
2. **Transaction Network Analysis (TNA):** As part of the EU's collective efforts, Malta has access to the TNA tool, an automated data mining system that interconnects Member States' tax IT platforms. This facilitates rapid access to cross-border transaction information, enabling near real-time detection and reporting of suspicious VAT activities.
3. **Cross-Border Cooperation:** Malta collaborates with other EU Member States through networks like Eurofisc, enhancing the exchange of information and coordination in tackling cross-border VAT fraud schemes. This cooperation is vital in dismantling complex fraud networks that operate across multiple jurisdictions.
4. **Financial Intelligence Analysis Unit (FIAU):** Malta's FIAU is responsible for collecting and analyzing financial intelligence related to money laundering and terrorism financing, which includes aspects of VAT fraud. The FIAU disseminates its findings to law enforcement agencies for further investigation and potential prosecution.

By leveraging these tools and fostering international cooperation, Malta aims to effectively detect, investigate, and prosecute VAT fraud, thereby safeguarding its fiscal interests and maintaining compliance with EU regulations.

¹⁵⁶ Article 637 C.C.P.

(1) Public prosecution resulting from a crime shall be time-barred after ten years have elapsed from the day on which the crime was committed, if no investigation or prosecution has been carried out in that interval. If, in the interval referred to in paragraph 1, acts of investigation or prosecution have been carried out which have not been followed by judgment, the prosecution shall not be time-barred until ten years have elapsed, from the date of the last act, even in respect of persons who are not involved in the act of investigation or prosecution.

(2) [...]

¹⁵⁷ Article 638 C.C.P.

In the cases set out in the preceding article, and in accordance with the distinctions of time established therein, the duration of the limitation period shall be reduced to five years if it is an offence of such a nature as to be punishable by correction.

According to the national expert, these tools can be improved by effectively **aligning criminal sanction procedures with administrative sanction procedures** abiding by the ‘una via’ principle. Criminal procedures would be justified only in cases meeting a materiality threshold.

About **jurisdiction**, in Malta, principles of personality and territoriality applies. According to Article 11, paragraph 4 of the PIF Directive, in cases where the personality principle applies, certain conditions are excluded: in Malta this condition is that the prosecution can be initiated only following a denunciation from the State of the place where the criminal offence was committed.

Regarding the **minimum limitation period** of at least 5 years provided by Article 12 of the PIF Directive, Malta is compliant [Article 688 Criminal Code¹⁵⁸].

The Netherlands

The Dutch authorities can rely on different investigative tools to fight against VAT fraud, for instance:

- **Requests for information**, including the surrender of books and administration, by the tax authorities or law enforcement authorities to the corporations involved.
- **Use of international requests for information** based on a simplified procedure for tax information exchange offered by the Standing Committee on Administrative Cooperation.
- **Requests for information from investigative authorities to banks** in order to provide the authorities with bank statements of the suspect.
- **Request for information from the Chamber of Commerce.**
- **Telephone tapping.**
- **Witness statements.**
- **Search (on premises of organisation) and seizure of books and administration.**
- **Interrogation of the suspect.**

These tools are useful also to fight cyber VAT fraud, also because, according to the national expert, it is very hard to imagine that there still is any non-cyber VAT fraud, at least if cyber VAT fraud is defined as broadly as is in this project. For example, the tax authorities only accept VAT declarations made through an online portal. Most cyber VAT offences will use digitized money transfer systems or banks, and use digital communication tools, which are all covered for investigatory purposes by the tools described above. Therefore, it is very unlikely that the tools available will not suffice to fight cyber VAT fraud as understood in the way described in this project.

During the focus groups, the expert stressed that while e-invoicing isn't an investigative tool per se, it is key to providing data for tax authorities to detect fraudulent activities. At the same time, the expert highlighted the importance of **combining criminal law with procedural tools** and emphasized the growing use of Big Data and AI tools to manage the overwhelming amount of data generated

¹⁵⁸ Art. 688 criminal code:

Save as otherwise provided by law, criminal action is barred- (d) by the lapse of five years in respect of crimes liable to imprisonment for a term of less than four years but not less than one year;

by e-invoicing and digitalization efforts. AI will be central in recognizing patterns and identifying fraud within these large datasets.

About **jurisdiction**, The Netherlands follows the principle of **dual criminality**, except for crimes defined in the PIF Directive, where the condition does not apply.

The Dutch legislation is **compliant with Article 12 of the PIF Directive on the limitation period**, providing one of at least 5 years.

In case of a penalty of more than one year of imprisonment and in case of a penalty of imprisonment for a criminal offense that is punishable by a maximum sanction of at least four years of imprisonment, a penalty imposed for VAT fraud can be enforced for at least five years from the date of the final conviction.

Poland

In Poland, the investigative tools against VAT fraud are foreseen in Section III b of the Tax Ordinance Act, specifically in the **General Anti-Avoidance Rule (GAAR)** - Art. 119zg-119zzk.

According to those articles, the **STIR (Standardized Tax Information Exchange System)** is one of the key systems to fight against VAT fraud, providing a technical framework to assess **financial transactions** and monitor the **flow of funds**. During the focus groups expert argued that digitalisation, in particular electronic invoices and traceability of payments, are essential for the detection of fraudulent VAT transactions and that they are therefore useful general investigation tools that must be digital in order to detect digital crimes.

Thus, the **Polish GAAR** employs tools such as **data analysis**, **financial monitoring systems** (like STIR), and direct **collaboration** with **banks** and **financial institutions** to investigate suspicious activities.

Against cyber VAT fraud it is possible to use effectively also tools in **Section IIIc of the Tax Ordinance - Anti-abuse of law in cross-border operations** - art. 119zzl-119zzs.

This Section is stressed out also the importance of the international cooperation.

About jurisdiction, in Poland it is applied the **principle of territoriality**. Indeed, VAT fraud falls under Polish jurisdiction when the criminal offense is committed in whole or in part within the country's territory, when the offender is a habitual resident in the territory, and when the criminal offense is committed for the benefit of a legal person established in the territory.

Poland is compliant with Article 12 of the PIF Directive on the **limitation period (at least 5 years)**.

Regarding the possibility of **enforcing for at least five years from the date of the final conviction sanction for VAT fraud**, Poland, as the majority of the responding MSs (Austria; Belgium; Croatia; Cyprus; Czech Republic; Hungary; Ireland; Romania; Sweden; The Netherlands), answered "both in case of a penalty of more than one year of imprisonment and in case of a penalty of imprisonment for a criminal offense which is punishable by a maximum sanction of at least four years of imprisonment".

Portugal

The Portuguese Tax Authority (Autoridade Tributária e Aduaneira - AT) publishes **annual reports on combating tax and customs fraud and evasion**. These reports provide detailed information on the measures implemented, results achieved, and ongoing challenges in the fight against tax fraud. In the last one, it is highlighted, **as a means of enforcement, the digitalization of tax processes and the collaboration of Portuguese entities with other European and national entities**. For instance, 180 Tax Authority workers participated in webinars on fraud detection promoted by the European Union Agency for Law Enforcement Training (CEPOL) in 2022.

To improve the current tools for **combating VAT fraud**, the report suggests the **use of new technologies, also based on AI systems**, capable of detecting fraudulent patterns, like the techniques that are being implemented by banks and financial intermediation firms in detecting money laundering, financial fraud, and terrorism financing. These technologies can enhance the ability to identify and prevent fraudulent activities more efficiently. Studies in Anti-Money Laundering (AML), indeed, suggest that AI can significantly reduce the number of false positives, enhancing the efficiency and accuracy of fraud detection processes.

As for the **jurisdiction** of VAT fraud, this crime falls under Portuguese jurisdiction when the criminal offense **is committed in whole or in part within the country's territory**.

Finally, **by Article 12 of the PIF Directive, the national legislation of Portugal does provide for a limitation period of at least 5 years** for the criminal offense of VAT fraud Art. 21, Lei 15/2001¹⁵⁹].

Romania

The Romanian tax authority, the National Agency for Fiscal Administration ("NAFA"), relies on **different tools to investigate tax fraud including VAT fraud**: NAFA directs and conducts tax audits and in case there is any suspicious element of a fraud the criminal prosecutor will be notified.

Currently, the tax audits have four different forms:

- Tax inspection.
- Unannounced check.
- Fraud check.
- Desk inspection.

Based on the information included in the Annual performance activity of NAFA for 2023 published on 25 March 2024, the **main tool used was tax inspection** with a total of 20,796 audits (15,610

¹⁵⁹ Article 21, Lei 15/2001:

Limitation, Interruption, and Suspension of Criminal Proceedings

1 - The criminal proceedings for a tax crime are extinguished by limitation once five years have elapsed since the act was committed.

2 - The provision in the preceding paragraph does not affect the limitation periods established in the Penal Code when the maximum limit of the prison sentence is five years or more.

3 - The limitation period for criminal proceedings is reduced to the expiration period of the right to assess the tax liability when the offense depends on that assessment.

4 - The limitation period is interrupted and suspended under the terms established in the Penal Code, but the suspension of the limitation also occurs due to the suspension of the proceedings, as provided in paragraph 2 of Article 42 and in Article 47.

legal persons and 5,186 natural persons). Additionally, the tax authority issued 270 notifications to the criminal prosecutor. NAFA has a specialized unit, the General Directorate for Tax Fraud (Direcția Generală Antifraudă Fiscală), which is dedicated to investigating tax fraud. This unit is also responsible for notifying the criminal prosecutor when fraud is identified. In 2023, the Directorate sent 199 notifications to the criminal prosecutor to initiate criminal investigations¹⁶⁰.

Furthermore, the tax authority employs several additional tools to combat tax fraud. These include the **exchange of information on request and the exchange of information without prior request**, in line with current EU legislation. According to the Annual Performance Activity Report of NAFA for 2023, published on 25 March 2024, Romania responded to 945 requests from other countries and sent 1,121 requests, based on agreements under Council Regulation (EU) No 904/2010 on administrative cooperation and combating VAT fraud. Additionally, under the Bilateral Agreement on administrative cooperation in VAT matters between NAFA and the Bulgarian National Revenue Agency (ANV), 47 requests for information were received, and 58 requests were sent to the Bulgarian tax authorities.

The tax authority also participates in multilateral controls (MLCs) conducted simultaneously across two or more EU Member States. This allows for **enhanced cooperation and the ability for tax officials to access documentation across borders**. Under the framework of the Community Instruments for Advanced International Administrative Cooperation (IAAC) and multilateral controls/PAOE1, NAFA coordinated six operations in 2023 to combat VAT fraud and direct taxes, specifically targeting areas such as transfer pricing, labor, cross-border advisory services, and intra-community transport services.

In Romania, **there are no specific investigative tools for cyber VAT fraud**.

According to the national expert, the current legal framework in Romania is sufficient to combat VAT fraud. However, **the main challenge lies with the tax authority, as the relevant data provided by taxpayers, service providers, and payment service providers is not being fully utilized**. The reporting obligations for businesses are already comprehensive, with the implementation of tools such as SAFT, e-invoicing, and digital reporting. The tax authority has access to this information, but the key issue is ensuring it is properly used.

During the focus groups, the expert emphasized Romania's commitment to driving maximum digitization. The country is implementing a wide range of digital tools, including e-VAT and e-SFT, to ensure that all taxpayers submit their tax returns digitally and electronically. The expert stressed that the tax authority must be able to effectively leverage this data to identify potential fraud and improve enforcement.

In Romania, both the territoriality and personality principles apply in determining jurisdiction. The **territoriality principle** allows Romanian criminal law to be applied to offenses committed within the country's territory, while the **personality principle** extends jurisdiction to crimes committed outside Romania by Romanian citizens or legal entities. This dual approach ensures that Romania has legal authority over a broad range of offenses, regardless of where they occur, as long as there is a connection to the country through territory or nationality¹⁶¹.

¹⁶⁰ Annual performance activity of NAFA for 2023 published on 25 March 2024.

¹⁶¹ In the Romanian criminal code, there are different dispositions related to the jurisdiction:

Art. 8:

Territoriality of criminal law

(1) Romanian criminal law applies to offences committed on the territory of Romania.

(2) The territory of Romania is defined as the expanse of land, the territorial sea waters and inland waters, complete with the soil, sub-soil and airspace located inside the national borders.

(3) An offence committed on the territory of Romania is defined as any offence committed on the territory defined at par. (2) or on a ship sailing under Romanian pavilion or on an aircraft registered in Romania.

(4) The offence is also considered as having been committed on the territory of Romania when on that territory or on a ship sailing under Romanian pavilion or on an aircraft registered in Romania an action was committed with a view to perform, instigate or aid in the offense, or the results of the offense have been manifested, even if only in part.

Art. 9:

Legal standing under criminal law

(1) Romanian criminal law applies to offences committed outside Romanian territory by a Romanian citizen or a Romanian legal person if the sentencing stipulated by Romanian law is life imprisonment or a penalty of more than 10 years imprisonment.

(2) In the other cases Romanian criminal law applies to offences committed outside Romanian territory by a Romanian citizen or a Romanian legal person if the act is also criminalized by the criminal law of the country where it was committed or if it was committed in a location that is not subject to any State's jurisdiction.

(3) A criminal investigation can start on receiving authorization from the Chief Prosecutor of the Prosecutor's Office attached to the Court of Appeals in whose jurisdiction the first Prosecutor's Office is located that received information about the violation, or, as the case may be, from the Prosecutor General of the Prosecutor's Office attached to the High Court of Review and Justice. A prosecutor is entitled to issue such authorization within 30 days of receiving the application for authorization; such deadline can be extended, under the law, but for no more than a total of 180 days.

Art. 10:

Reality of criminal law

(1) Romanian criminal law applies to offences committed outside Romanian territory by a foreign citizen or a stateless person against the Romanian State, against a Romanian citizen or against a Romanian legal person.

(2) A criminal investigation can start on receiving authorization from the Prosecutor General of the Prosecutor's Office attached to the High Court of Review and Justice, and only if the violation is not the object of judicial procedures that are already ongoing in the State on whose territory it was committed.

Art. 11:

Universality of criminal law

(1) Romanian criminal law also applies to other violations than those stipulated at Art. 10, committed outside Romanian territory by a foreign citizen or a stateless person who is located voluntarily on Romanian territory, in the following cases:

a) an offence was committed that the Romanian State has undertaken to repress on the basis of an international treaty, irrespective of whether it is stipulated by the criminal law of the State on whose territory it was committed.

b) extradition or surrender of the offender has been requested and denied.

(2) The stipulations of par. (1) b) do not apply when, under the law of the state on whose territory the violation was committed, there is a cause to prevent the start of criminal action or the continuing of the criminal trial or the serving of the sentence or when the sentence has been served or when the sentence is considered as having been served.

(3) When the sentence has not been served or has only been served in part, the applicable procedure is that of the law on the recognition of foreign judgments.

Additionally, Article II Law 234/2022 transposed Art. 11 (1) (b) PIF Directive:

By way of derogation from the provisions of Article 9 of Law no. 286/2009 on the Criminal Code, with subsequent amendments and completions, as well as in the application of Article 12 of the same law, if the facts are committed outside the territory of the country by a Romanian citizen or a Romanian legal person, regardless of the punishment stipulated by the Romanian law, even if the act is not stipulated as a criminal offence by the criminal law of the country where it was committed and without the prior authorization of the prosecutor general from the prosecutor's office attached to the court appeal in whose territorial area is the prosecutor's office first notified or the prosecutor general from the prosecutor's office attached to the High Court of Cassation and Justice, the Romanian criminal law applies to the offences stipulated in:

a) Articles 6, 7 and 18¹-18⁵ of Law 78/2000 for the prevention, discovery and sanctioning of corruption deeds, with subsequent amendments and completions.

b) Art. 4, 8 and 9 of Law 241/2005 for the prevention and combating of tax evasion, with subsequent amendments and completions, art. 270 and art. 272-275 of Law 86/2006 regarding the Customs Code of Romania, as amended and supplemented, art. 289-292, art. 294, 295, 297, 298, art. 306-309 and art. 367

Romania is compliant with Article 12 of the PIF Directive on the **limitation period (at least 5 years)**.

In Romania, a **penalty imposed for VAT fraud can be enforced for at least five years from the date of the final conviction** in case of a penalty of more than one year of imprisonment and in case of a penalty of imprisonment for a criminal offense which is punishable by a maximum sanction of at least four years of imprisonment.

Slovakia

The investigative tools used to combat VAT fraud in Slovakia **include the mandatory submission of VAT tax returns electronically and the monthly VAT statements**. While these tools can be applied to detect cyber VAT fraud, their effectiveness remains questionable, as there are currently **no specific investigative tools dedicated to addressing this form of fraud**.

Regarding **jurisdiction**, the **principle of territoriality** applies: indeed a fact falls under Slovakian jurisdiction when the criminal offense is committed, in whole or in part, within Slovakia's territory. Additionally, jurisdiction **extends when the offender is one of the country's officials acting in their official capacity**.

Slovakia's legal framework is **compliant with Article 12 of the PIF Directive**, as it establishes a limitation period of at least five years for VAT fraud cases. According to national legislation, a penalty imposed for VAT fraud can be enforced for at least five years from the date of the final conviction, specifically in cases where the criminal offense is punishable by a maximum sanction of at least four years of imprisonment.

Slovenia

Even though Slovenia did not respond to the questionnaire prepared for the EU Cyber VAT fraud project, it has nonetheless been possible to analyse the investigative legal framework on VAT fraud in Slovenia.

In Slovenia, combating VAT fraud involves a combination of investigative tools and legal provisions aimed at detecting and preventing fraudulent activities. Key tools and measures include:

- **Electronic VAT Returns and Digital Reporting:** Starting this June, businesses will be required to submit VAT tax returns electronically, facilitating efficient data collection and analysis by tax authorities.
- **Regular Audits and Inspections:** Tax authorities conduct audits and inspections to verify the accuracy of VAT declarations and identify discrepancies indicative of fraudulent activities.
- **Search and Seizure Operations:** Authorities have the legal mandate to perform searches and seize documents or assets related to suspected VAT fraud, enhancing their ability to gather evidence.

of the Law 286/2009 on the Criminal Code, with its subsequent amendments and completions, and Article 49 of the Law 129/2019 for the prevention and combating of money laundering and terrorist financing, as well as, as well as for the modification and completion of some normative acts, with subsequent amendments and completions, if they have resulted in the achievement of the financial interests of the European Union.

- **Interviews and Surveillance:** Investigative procedures include conducting interviews with suspects and employing surveillance techniques to monitor activities linked to VAT fraud schemes.
- **Inter-Agency Collaboration:** Cooperation among various governmental bodies, such as tax authorities, customs, police, and the judiciary, is crucial for effective detection and prosecution of VAT fraud.
- **Use of Advanced Technologies:** Slovenia is exploring the implementation of artificial intelligence and digital tools to analyze large datasets, aiming to identify suspicious patterns and anomalies in VAT transactions.

While Slovenia utilizes these general investigative tools, there are **no specific instruments exclusively dedicated to cyber VAT fraud**. The effectiveness of existing tools in addressing cyber VAT fraud is an area under continuous evaluation.

Regarding legal **jurisdiction**, Slovenian criminal law applies based on the **territoriality principle**, meaning it covers offenses committed wholly or partially within Slovenia's territory. Additionally, Slovenian law extends to offenses committed abroad by Slovenian citizens or legal entities, provided the act is also criminalized in the country where it was committed.

Slovenia is compliant with Article 12 of the PIF Directive on the **limitation period** (five years after the date when the tax was due; ten years is the absolute limitation period).

Spain

The authorities in Spain that can carry out investigations related to VAT fraud are as follows:

- **Tax Agency (AEAT)**, specifically the **Inspection Authorities** and **National Fraud Investigation Office**.
- **Customs Surveillance Service**.
- **Prosecutor's Office specialized in economic crimes**.
- **Prosecutor's Office specialized in IT crimes**.
- **European Public Prosecutor's Office:** Although the European Public Prosecutor's Office (EPPO) is generally not competent to investigate VAT fraud as it is a national tax matter, it can intervene when the case involves at least two Member States and results in damages exceeding 10 million euros.
- **Specialized Units of the National Police:** These include the **Central Unit for Economic and Tax Crime** and the **Central Brigade for Technological Investigation (BCIT)**.

Regarding the tools used by these authorities to detect and combat VAT fraud, it has to be noted that the Tax Agency (AEAT) and the Tax Inspection Authorities have their own operational program. However, for reasons of confidentiality and the agency's operational capacity, no further data on its functioning is published. The same is true for Customs Surveillance Service.

Other tools are:

- **OSforensics:** This is a digital forensic tool used in tax fraud investigations to analyze computer systems for digital evidence. It helps identify files, records, electronic

communications, and data manipulations linked to VAT fraud. OSforensics supports legal proceedings by providing essential digital evidence.

- **HASH:** The HASH tool is used to verify the integrity of financial data by generating unique fingerprints for relevant files. These fingerprints are then compared with those obtained during the investigation to detect tampering or unauthorized changes in documents, financial records, or tax returns that may indicate fraudulent activity.

Currently, **there are no specific tools identified for investigating cyber VAT fraud.**

To improve the detection and prosecution of VAT fraud, **several changes are recommended:**

- **Create Specialized Judges or Courts for Economic Crimes:** Although Spain has specialized prosecutor's offices for economic and IT crimes, judges lack the necessary training to handle these complex cases effectively. This lack of specialized judicial training in economic crimes, including VAT fraud, poses a significant obstacle to effective prosecution. This issue also affects the prosecution of other complex crimes like organized crime and environmental crimes.
- **Changes to the Procedural Model:** It is suggested that Spain adopts a pure accusatory model in which the prosecutor leads criminal investigations rather than the investigating judge. This change would give prosecutors the authority to decide whether or not to pursue charges after investigating the case. Currently, while there are specialized economic crime and cybercrime units in the Public Prosecutor's Office, there are no corresponding specialized units in the judiciary.
- **Reform of Criminal Procedural Law:** Spain's Criminal Procedure Law, dating back to 1882, needs a comprehensive reform to modernize and speed up investigation procedures. Some specific areas require attention:
 - **Maximum Investigation Periods:** The 12-month limit set by Article 324 of the Criminal Procedure Act is too short to investigate complex economic crimes like VAT fraud. An extension of this period is necessary for such cases.
 - **Pre-trial Appeals System:** The current system allows almost all decisions issued by the investigating judge to be appealed. This often leads to delays. A new procedural model, where the prosecutor conducts the investigation and decides whether to bring charges, would streamline the process. Appeals could then occur between the investigation and trial stages.
 - **Processing Separate Pieces of Evidence in Macro-Cases:** The delays in processing large cases (macro-cases) due to their complexity hinder the investigation and prosecution of economic crimes. A more efficient way to handle evidence in macro-cases could improve the speed of legal proceedings.

Spain's **jurisdiction** for VAT fraud cases is governed by the principles of **territoriality** and **personality**:

- The **territoriality principle** applies when the criminal offense occurs entirely or partially within Spanish territory and when the VAT fraud benefits a legal person established in the country¹⁶².

¹⁶² In accordance with article 31 bis of the Penal Code, which contains the system of criminal liability of legal entities. See footnotes 108 and 109.

- The **personality principle** applies when the offender is Spanish¹⁶³ or a Spanish official acting within their official capacity¹⁶⁴.

If the VAT fraud offense is committed by a Spanish citizen outside Spain, Spanish jurisdiction applies under the conditions set out in Article 23.2 of the Ley Orgánica 6/1985, of 1 July 1985¹⁶⁵ (The Judiciary Act).

In Spain, VAT fraud penalties can be enforced for **at least five years** from the date of the final conviction under certain conditions (Art. 31 C.C.¹⁶⁶). Article 33.3(a) of the Spanish Criminal Code defines prison sentences of 3 months to 5 years as less serious penalties. VAT fraud typically falls within this category, and thus the penalties for tax crimes can be enforced within five years of the final conviction. In the case of **aggravated VAT fraud**, the time limit for enforcement may be longer¹⁶⁷.

¹⁶³ Art. 23.1 of the Ley Orgánica 6/1985, of 1 July 1985, of the Judiciary:

“1. In criminal matters, Spanish jurisdiction shall be competent to hear cases involving crimes and misdemeanors committed in Spanish territory or committed on board Spanish ships or aircraft, without prejudice to the provisions of international treaties to which Spain is a party”.

¹⁶⁴ Art. 23.3.h of the Ley Orgánica 6/1985, of 1 July 1985, of the Judiciary:

“3. Spanish jurisdiction shall be competent for acts committed by Spaniards or foreigners outside the national territory when they are liable to be classified, according to Spanish criminal law, as any of the following offences:

h) Those perpetrated in the exercise of their functions by Spanish public officials residing abroad and crimes against the Spanish Public Administration”.

Section 6 of article 23 of the Ley Orgánica 6/1985, of 1 July 1985, of the Judiciary states a condition:

“6. The offences referred to in paragraphs 3 and 4 shall only be prosecutable in Spain after a complaint has been lodged by the aggrieved party or by the Public Prosecutor's Office”.

¹⁶⁵ Article 23.2 of the Ley Orgánica 6/1985, of 1 July 1985 (The Judiciary Act):

2. Spanish jurisdiction shall also be exercised over offences committed outside the national territory, provided that those criminally responsible are Spanish nationals or foreigners who have acquired Spanish nationality after the commission of the act and that the following requirements are met:

a) That the act is punishable in the place of execution, unless, by virtue of an international treaty or a regulatory act of an international organisation to which Spain is a party, this requirement is not necessary, without prejudice to the provisions of the following paragraphs.

b) That the aggrieved party or the Public Prosecutor's Office files a complaint with the Spanish courts. This requirement shall be deemed to be met in relation to offences within the jurisdiction of the European Public Prosecutor's Office when the latter actually exercises its jurisdiction.

c) That the offender has not been acquitted, pardoned or sentenced abroad, or, in the latter case, has not served the sentence. If he has only served it in part, it shall be taken into account in order to reduce his sentence proportionally”.

¹⁶⁶ Art. 31 of the Spanish Criminal Code:

1. The statute of limitations for offences shall expire:

At twenty years, when the maximum penalty indicated for the offence is imprisonment for fifteen years or more.

At fifteen years, when the maximum penalty established by law is disqualification for more than ten years, or imprisonment for more than ten but less than fifteen years.

At ten, where the maximum penalty prescribed by law is imprisonment or disqualification for more than five years and not exceeding ten years.

At five, for all other offences, except less-serious offences and the offences of libel and slander, which are subject to the statute of limitations after one year.

¹⁶⁷ Article 133 of the Spanish Criminal Code:

1. The penalties imposed by final judgement are subject to the statute of limitations: (...) At five years, the less serious penalties.

Therefore, the penalties for a tax crime may be executed within 5 years of the final conviction.

In the case of an aggravated tax offence, the time limit may be longer.

Sweden

In Sweden, to combat VAT fraud, the following investigative tools are used:

- **Secret Coercive Measures:** These are covert measures employed by authorities to gather evidence and conduct investigations, often without the knowledge of the subjects involved. These measures include:
 - **Telephone Surveillance:** Secret surveillance of electronic communication, which records the details of telephone calls (such as who called, when, and for how long), but not the content of the conversations.
 - **Camera Surveillance:** The use of hidden cameras to monitor individuals or premises in connection with the investigation.
 - **Room Surveillance:** Covert monitoring of rooms to capture activity and conversations.
 - **Secret Monitoring of Electronic Communication:** This includes obtaining information on electronic communications, such as emails or messages, to trace potentially fraudulent activity.
 - **Secret Data Reading:** This new, time-limited measure, introduced on April 1, 2020, allows authorities to read data stored electronically to uncover evidence of tax fraud or related criminal activities.

In addition to these secret coercive measures, **ordinary coercive measures** can also be used, such as:

- **Seizure** of assets and records.
- **Detention, arrest, and remand** of suspects.
- **House searches** for relevant evidence.

Cyber VAT fraud can be challenging to investigate, but the application of **secret coercive measures** such as telephone surveillance, camera surveillance, and secret data reading can be effective. These tools allow authorities to collect critical digital evidence while maintaining the confidentiality of the investigation. Although there were earlier difficulties in seizing data stored in cloud systems, recent legislative changes have addressed this gap, enhancing the ability to combat cyber VAT fraud.

The national expert suggests that while the existing tools are quite effective, further improvements could be made, including:

- **Increased use of Artificial Intelligence (AI):** The Swedish Economic Crime Authority (SECA) has seen success in using AI to analyze large datasets for suspicious patterns. Expanding AI tools could provide better fraud detection capabilities, especially in large and complex VAT fraud cases.
- **Faster and Greater Access to Financial Information:** Timelier access to financial data from third parties, such as banks and financial institutions, would significantly improve the speed and accuracy of VAT fraud investigations.
- **Stronger Inter-Agency Collaboration:** A closer collaboration and better information exchange between relevant authorities, including tax agencies, law enforcement, and financial institutions, would improve the overall effectiveness of VAT fraud investigations.

VAT fraud falls under the **jurisdiction** of Swedish legislation in the following circumstances:

- **When the offense is committed wholly or partially within the country's territory.**
- **When the offender is of the country's nationality.**
- **When the offender is a habitual resident of the country**, particularly when the offense could lead to a prison sentence of six months or more.
- **When the criminal offense is committed for the benefit of a legal person established in the country**, such as in cases involving bribery or corruption.

It must be noted that the principle of **double criminality applies**: the offense must be recognized as a crime in both jurisdictions.

Sweden complies with **Article 12 of the PIF Directive** concerning the **limitation period** for criminal offenses.

Under national law, penalties for VAT fraud can be enforced for at least five years from the date of the final conviction in the following circumstances:

- **Fines and Imprisonment for up to 1 Year:** The limitation period is five years for cases involving fines or imprisonment for up to one year.
- **Imprisonment for 1-4 Years:** The limitation period extends to **10 years** for sentences ranging from 1 to 4 years of imprisonment.
- **Imprisonment for 4-8 Years:** The limitation period is **15 years** for sentences ranging from 4 to 8 years.
- **Imprisonment for More than 8 Years:** The limitation period extends to **20 years** for sentences of more than 8 years.
- **Life Sentences:** In cases where the sentence is for life imprisonment, the limitation period extends to **30 years**.

6. E-commerce and cooperation between the public and private sectors to combat and prevent cyber-VAT fraud

The development of electronic commerce (e-commerce) has enabled individuals and businesses to buy and sell an increasing volume of both physical and digital goods, as well as services, electronically. However, this growth comes with a heightened risk of tax evasion and fraud.

The final section of the legal analysis examines how **EU Directive 2020/284** and the **VAT Mini One Stop Shop (MOSS) scheme** are implemented at the national level to combat VAT fraud in the context of e-commerce.

According to EU directives, particularly the **EU VAT Directive (2006/112/EC)**, there are **three types of e-commerce**:

- **Business-to-Consumer (B2C) E-Commerce:** This involves transactions where a business sells goods or services directly to consumers. For VAT purposes, this is important because it determines the place of taxation and compliance requirements. Under the EU VAT rules, businesses engaged in B2C e-commerce are subject to VAT in the member state where the goods or services are consumed.
- **Business-to-Business (B2B) E-Commerce:** This type refers to transactions where businesses sell goods or services to other businesses. B2B transactions are usually subject to VAT in the country where the buyer is located, and the reverse-charge mechanism can be applied in certain cases, particularly within the EU.
- **Consumer-to-Consumer (C2C) E-Commerce:** This refers to transactions between consumers, often facilitated by online platforms. While these transactions are typically exempt from VAT, the role of the platform provider may require compliance with VAT obligations if they act as intermediaries in facilitating the sale of goods or services.

In addition to these, the **EU VAT Directive** also recognizes the role of **online marketplaces** that facilitate the sale of goods between sellers and buyers. These platforms may have specific VAT obligations under the "Marketplace VAT" rules introduced by the EU in 2021. This includes obligations to collect and remit VAT for sales facilitated on their platform, even if they are not directly involved in the sale.

The development of electronic commerce (e-commerce) has enabled individuals and businesses to buy and sell an increasing volume of both physical and digital goods, as well as services, electronically. However, this growth comes with a heightened risk of tax evasion and fraud.

VAT fraud in e-commerce can take various forms exploiting the complexity of cross-border transactions and online sales. For instance:

- **Non-registration for VAT.**
 - **Non-EU online sellers** may sell goods or services to EU consumers without registering for VAT anywhere in the EU. This allows them to avoid charging and remitting VAT to EU tax authorities.

- Some EU-based sellers may also fail to register for VAT, despite exceeding the VAT registration threshold in the country where they are selling.
- **Underreporting sales.**
 - **False reporting:** underreport the actual value of their sales to reduce the amount of VAT they are required to remit.
 - **Falsified invoices:** invoices with false information, such as incorrect sales amounts, to avoid paying the correct VAT.
- **Fraudulent VAT numbers.**
 - **Use of invalid VAT number.**
 - **Omission of VAT number on invoices.** Even when sellers display European business addresses and VAT numbers on their websites, these details are often omitted from the issued invoices because they are fraudulent.

As **e-commerce continues to grow, legislation and measures aimed at reducing the risks of fraud are also constantly evolving.** The European Commission has introduced several VAT and customs packages.

These new rules target payment service providers (PSPs), such as banks, payment institutions, and postal giro services, which collectively handle the majority of online transactions within the EU. The Organisation for Economic Co-operation and Development (OECD) has already emphasized the important role that platforms and PSPs can play in ensuring the effective enforcement of VAT regulations in the e-commerce sector. For this reason, the measures are increasingly aimed at holding these players accountable.

6.1 Digital marketplaces and the liability of providers

Regarding **service providers** in e-commerce, the EU has specific rules for digital services under **Directive 2008/8/EC**, which amended the VAT Directive. The definition of "digital services" includes a wide range of electronically supplied services, such as:

- Telecommunications services.
- Broadcasting services.
- Electronic services (e.g., streaming, e-books, software downloads).

For **e-commerce service providers**, the VAT rules depend on the nature of the service and where it is consumed. If a service is provided to a consumer within the EU, the VAT rules require the supplier to charge VAT based on the consumer's location, not the location of the service provider. This is part of the EU's efforts to simplify the VAT process for cross-border digital services, especially under the **Mini One-Stop Shop (MOSS)** scheme, which allows businesses to register in one EU member state and report VAT for sales to customers in other member states.

In general, service providers involved in e-commerce are subject to VAT obligations according to the type of service, the location of the customer, and whether they are selling to businesses or consumers.

This section of the analysis focuses on the obligations of payment service providers (PSPs) and explores mechanisms to enhance their role in detecting and preventing fraud. This section aims to assess how national laws align with EU directives on VAT fraud in e-commerce, the effectiveness

of current mechanisms for PSP compliance, and the potential for stronger involvement of payment and service providers in combating VAT fraud.

A specific event (the second online focus group) was dedicated to this discussion topic.

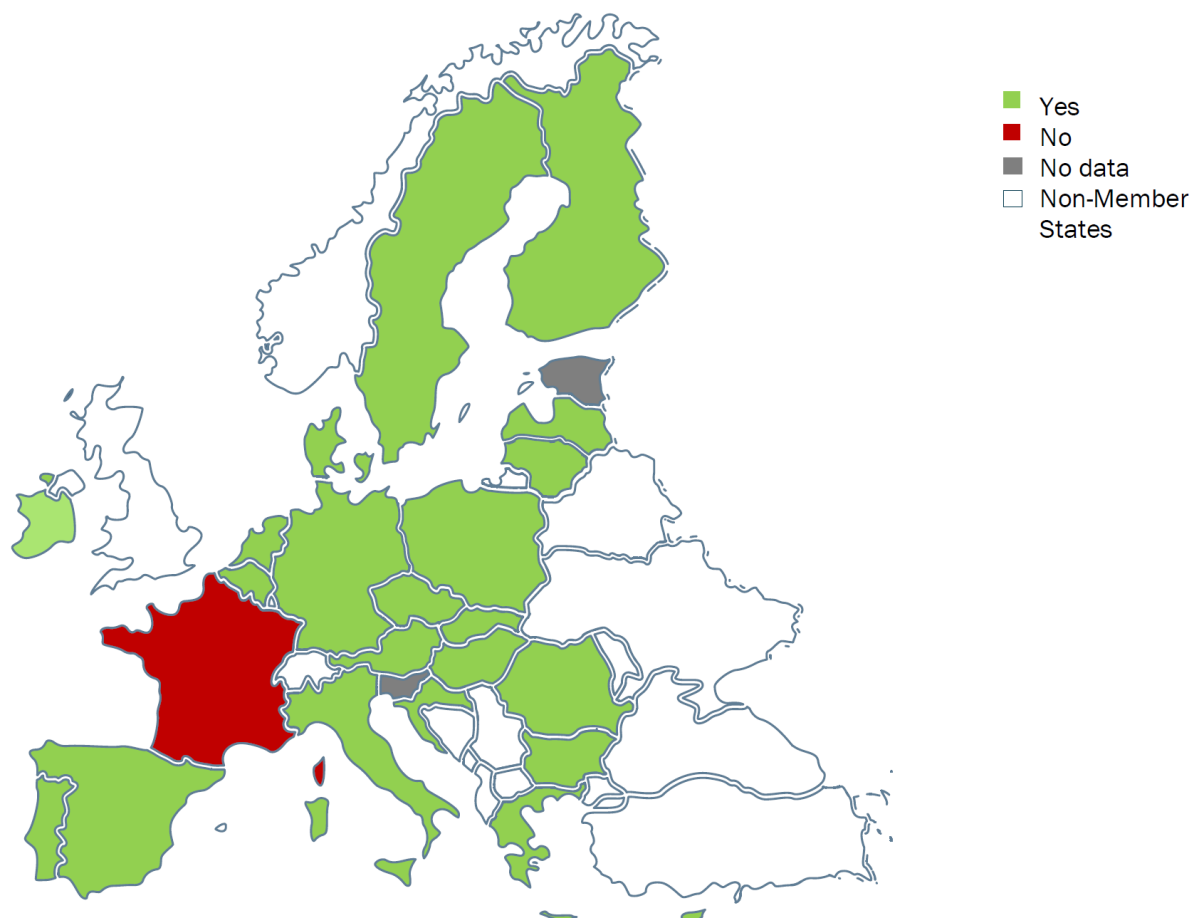
Based on the national responses to the questionnaire, participants were invited to discuss the **legal framework for VAT fraud** (and in particular missing trader intra-community (MTIC) fraud) in **e-commerce** in the Member States in the light of the introduction of new forms of **obligations for payment service providers to prevent VAT fraud** and assess the need for and impact of greater harmonisation in the regulation of cross-border VAT fraud, especially when it occurs in the context of e-commerce.

In particular, reference was made to MTIC VAT fraud in the digital market, the **role and responsibility of platforms** (both from the point of view of obligations and subjective elements) were discussed and finally, considerations were made on the transition from MOSS to the new OSS system.

Directive EU 2020/284 introduces new rules for payment service providers (PSPs) to fight VAT fraud in e-commerce. It requires PSPs to record and report details of cross-border payments within the EU, keeping detailed records of the payer, payee, and transaction data, which can be shared with tax authorities to monitor VAT compliance.

All MSs are compliant with **EU Directive 2020/284**, except France.

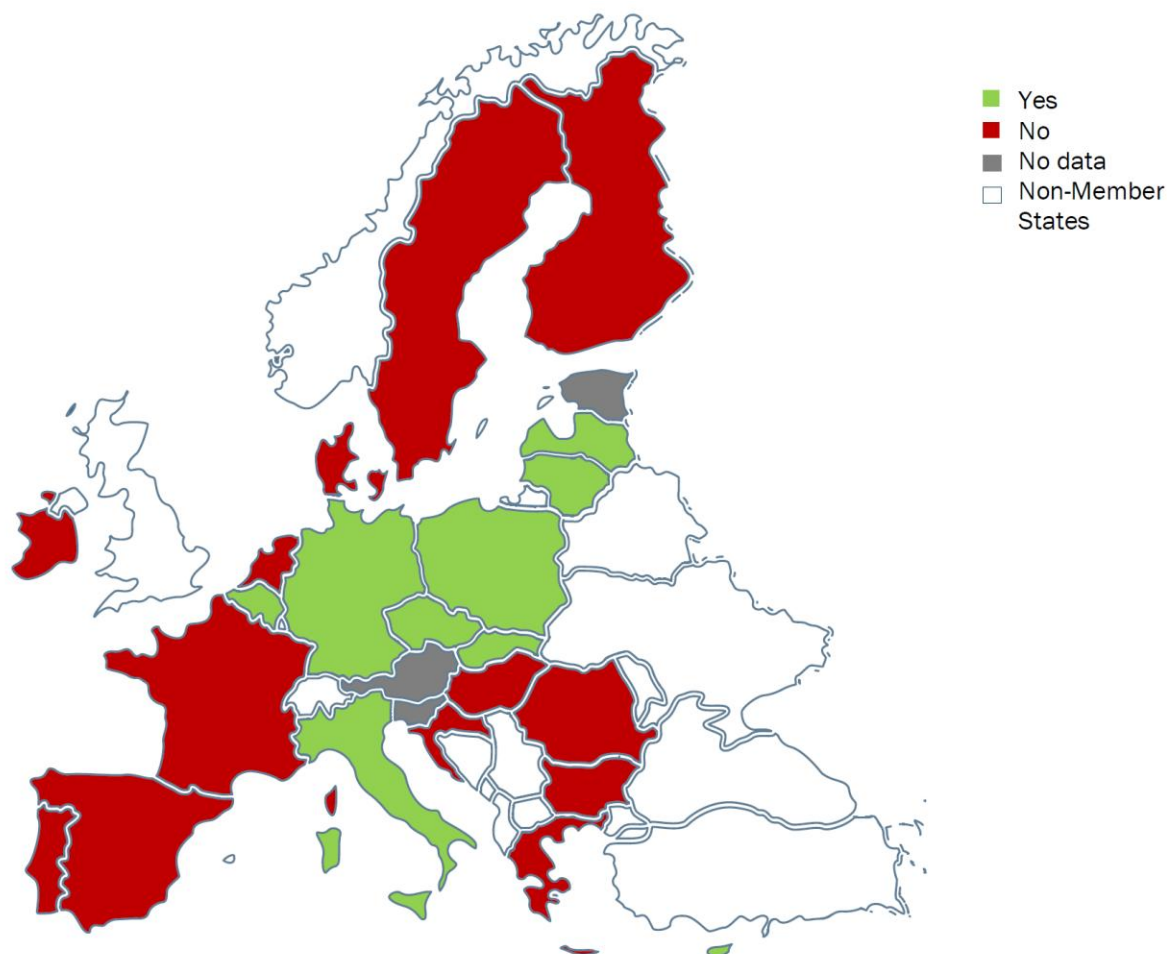
Fig. 19. Answer to question 17: “Is the national law of your country compliant with EU Directive 2020/284 Directive regarding the general obligations of payment service providers?” EU Member States. N=25. Year 2024.



Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

Most of the responding MSs (15: **Bulgaria, Croatia, Denmark, France, Finland, Greece, Hungary, Italy, Ireland, Luxembourg, Portugal, Romania, Spain, Sweden, and The Netherlands**) did not already have recording/reporting obligations for PSPs in place before the implementation of Directive 2020/284. However, 9 MSs had already established such requirements (Fig. 20).

Fig. 20. Answer to question 18: “Directive EU 2020/284 introduces new obligations for payment service providers in relation to the recording and reporting of payment information for cross-border payments as part of the European Union’s action plan to combat VAT fraud in e-commerce. Were these recording/reporting obligations already provided for in your national legislation?” EU Member States. N=25. Year 2024.



Source: elaboration by CSSC – project EU CYBER VAT – questionnaire for National Experts.

With regard to the sanctions foreseen in case of violation of PSPs’ obligations, the responses to this question reveal **a range of administrative and criminal penalties, fines, and legal repercussions**. Commonly, the amount of which depends on the severity and frequency of the offense. Here is a summary of the sanctions imposed by the responding MSs:

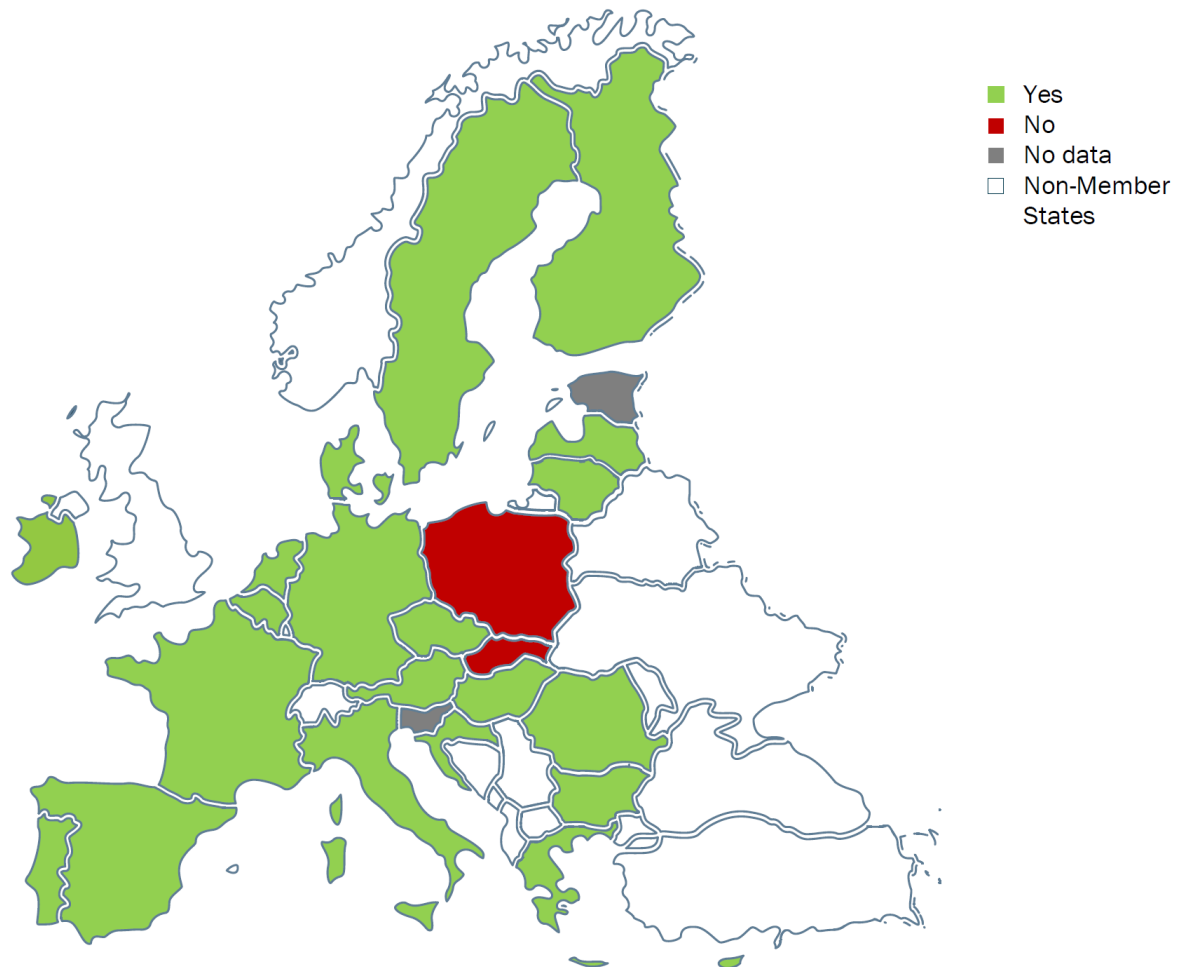
The common feature of these countries is the imposition of fines, with the amount of the fine varying depending on the type and frequency of the offense. Some countries also provide for non-monetary sanctions, such as imprisonment or public listing of non-compliant companies. The differences lie in the specific amounts and the additional sanctions for continued non-compliance.

The most important aspects are the financial implications and the emphasis on administrative sanctions to enforce compliance.

Almost all MSs have introduced the MOSS scheme, except for **Poland** and **Slovakia**.

In most cases, services previously covered under MOSS are now covered by the One Stop Shop (OSS).

Fig. 21. Answer to question 20: “The VAT Mini One Stop Shop (MOSS) is an optional scheme that allows you to account for VAT, which is normally due in multiple EU countries, in just one EU country. Has your country introduced the MOSS scheme?” EU Member States. N=25. Year 2024.



Source: elaboration by CSSC – project EU CYBER VAT

6.2 National legislations

Austria

Austria has transposed the EU Directive 2020/284 Directive regarding the general obligations of payment service providers¹⁶⁸ and at the same time has adopted the MOSS scheme.

Belgium

Belgium has transposed the EU Directive 2020/284 Directive regarding the general obligations of payment service providers¹⁶⁹.

Belgium is compliant also to Directive EU 2020/284, which introduces new obligations for payment service providers in relation to the recording and reporting of payment information for cross-border payments as part of the European Union's action plan to combat VAT fraud in e-commerce. These obligations already existed in the national legislation to a certain extent, but only for banks [Art. 93 *duodecies* VAT Code]. In 2019, these obligations were removed from the VAT Code. With the implementation of the Directive (EU) 2020/284, new provisions were introduced by the Act of 7 April 2023 amending the VAT Code regarding the introduction of certain recording and reporting obligations for payment service providers [Articles 93 *duodecies* and following of the VAT Code¹⁷⁰]. The obligations entered into force on 1 January 2024.

¹⁶⁸ Transposed by: Bundesgesetz, mit dem das Umsatzsteuergesetz 1994, die Bundesabgabenordnung, das Finanzstrafgesetz und das Bankwesengesetz hinsichtlich der Meldung von Zahlungsdaten durch Zahlungsdienstleister geändert werden (CESOP-Umsetzungsgesetz 2023).

¹⁶⁹ Art. 93 *duodecies* and following of the VAT Code.

¹⁷⁰ Art. 93 *duodecies*:

For the application of this chapter, the following terms shall mean:

1° “payment service provider”: one of the categories of payment service providers referred to in Article 1, para. 1, points a) to d) of Directive (EU) 2015/2366, or a natural or legal person enjoying an exemption under Article 32 of that Directive.

2° “payment service”: any of the business activities described in Annex I, in points 3 to 6 of Directive (EU) 2015/2366.

3° “payment”: subject to the exclusions referred to in Article 3 of Directive (EU) 2015/2366, a “payment transaction” as referred to in Article 4, point 5) of that Directive or a “money transfer” referred to in Article 4, point 22) of that Directive.

4° “payer”: a “payer” as referred to in Article 4, point 8) of Directive (EU) 2015/2366.

5° “payee”: a “payee” as referred to in Article 4, point 9) of Directive (EU) 2015/2366.

6° “home Member State”: the “home Member State” as referred to in Article 4, point 1) of Directive (EU) 2015/2366.

7° “host Member State”: the “host Member State” as referred to in Article 4, point 2) of Directive (EU) 2015/2366.

8° “payment account”: a “payment account” as referred to in Article 4, point 12) of Directive (EU) 2015/2366.

9° “IBAN”: “IBAN” as referred to in Article 2, point 15) of Regulation (EU) No 260/2012.

10° “BIC”: “BIC” as referred to in Article 2, point 16) of Regulation (EU) No 260/2012.’

Art. 93 *duodecies*/1:

§ 1. Payment service providers shall keep records of payees and payments relating to payment services they provide for each calendar quarter to enable the competent authorities of the Member States to carry out checks on supplies of goods and services deemed to take place in a Member State in accordance with the provisions of Title V of Directive 2006/112/EC in order to achieve the objective of combating VAT fraud.

§ 2. The obligation referred to in paragraph 1 shall apply only under the following conditions:

1° the payment services provided are related to cross-border payments.

2° the payment service provider provides payment services relating to more than twenty-five cross-border payments to the same payee in the course of a calendar quarter.

For the purposes of 1°, a payment shall be considered a cross-border payment if the payer is located in a Member State and the payee is located in another Member State, in a third territory or in a third country.

For the purposes of 2°, the number of cross-border payments shall be calculated on the basis of the payment services provided by the payment service providers per Member State and per identifier referred to in Article 93duodecies/2, paragraph 2. If the payment service provider has information that the payee has several identification codes, the calculation shall be made per payee.

§ 3. The obligation set out in paragraph 1 shall not apply to payment services provided by the payer's payment service providers for each payment where at least one of the payee's payment service providers is located in a Member State if this is evidenced by that payment service provider's BIC or other business identifier that unambiguously identifies the payment service provider and its location. The payer's payment service providers shall nevertheless take those payment services into account for the calculation referred to in § 2, paragraph 1, 2° and paragraph 3.

§ 4. Where the obligation referred to in paragraph 1 applies, the registers shall be:

1° kept in electronic form by the payment service provider and retained for a period of three calendar years from the end of the calendar year of the payment date.

2° in accordance with Article 24ter of Regulation (EU) No 904/2010, made available to the administration in charge of value added tax to enable it to fulfil its obligations arising from paragraph 3 of that provision, when:

a) Belgium is the home Member State of the payment service provider;

b) Belgium is the payment service provider's host Member State, where Belgium is not its home Member State but it provides payment services in Belgium.'

Art. 93duodecies/2:

'For the application of Article 93duodecies/1, § 2, paragraph 2, and without prejudice to the provisions of Title V of Directive 2006/112/EC, the location of the payer shall be deemed to be in the Member State corresponding to:

1° the IBAN of the payer's payment account or any other identifier which unambiguously identifies the payer and specifies the location of the payer;

2° in the absence of an identifier referred to in 1°, the BIC or any other business identifier which unambiguously identifies the payment service provider acting on behalf of the payer and specifies the location of the payment service provider.

For the application of Article 93duodecies/1, §2, (2), and without prejudice to the provisions of Title V of Directive 2006/112/EC, the location of the payee shall be deemed to be in the Member State corresponding to:

1° the IBAN of the payee's payment account or any other identifier that unambiguously identifies the payee and specifies the location of the payee;

2° in the absence of an identifier referred to in 1°, the BIC or any other business identifier which unambiguously identifies the payment service provider acting on behalf of the payee and specifies the location of the payment service provider.'

Art. 93duodecies/3:

'The registers referred to in Article 93duodecies/1, § 1 shall contain the following information:

1° the BIC or any other business identifier that unambiguously identifies the payment service provider;

2° the name or business name of the payee as it appears in the records of the payment service provider;

3° if available, a VAT identification number or other national tax number of the payee;

4° the IBAN or, if not available, any other identifier that unambiguously identifies the payee and gives the location of the payee;

5° the BIC or any other business identifier that unambiguously identifies the payment service provider acting on behalf of the payee and gives the location of the payee's payment service provider, if the payee receives funds without having a payment account;

6° if available, the address of the payee as it appears in the records of the payment service provider;

7° the details of each cross-border payment referred to in Article 93duodecies/1, § 2, paragraph 1, 1°;

8° the details of any refunds identified as being related to the cross-border payments referred to in 7°.

The information referred to in paragraph 1, 7° and 8°, shall contain the following details:

1° the date and time of the payment or refund;

2° the amount and currency of the payment or refund;

In case of a breach of the VAT Code, various fines are foreseen.

These sanctions are laid down in Article 5 of the Annex to the Royal Decree nr. 44 of 9 July 2012 setting the amount of non-proportional tax fines on value added tax. This legal provision states: €3,000 for first violation related to the correct keeping of the register and increasing amounts for subsequent violations; second violation: € 4,000; subsequent violations: 5,000€.

Failure to comply with the format or with the retention period of the register: 1,000€. If the register does not contain one or more entries or contains incomplete or incorrect entries, a minimum and a maximum monetary penalty are provided, which increases in the case of repeat offenses.

Lastly, there are also various monetary penalties for failure to notify (EUR 2,000 per unnotified piece of information), delayed (EUR 300 per notification per month of delay with a maximum of 3,000 EUR), or incorrect notifications (purely accidental irregularities: 80 EUR; other irregularities: 500 EUR).

Belgium has adopted the MOSS Scheme, now substituted with the OSS Scheme.

Finally, Q. 21 of the questionnaire, requested an opinion from the national expert on how could service providers and payment service providers be more involved in the detection and prevention of criminal offenses related to VAT fraud. The Belgian expert answered that **payment service providers are already quite involved in providing information to the authorities**. Before implicating these providers even more in the detection and prevention process, a more pressing question is probably **how to adequately and effectively process all this information**.

Bulgaria

Bulgaria **fully complies with EU Directive 2020/284** regarding the general obligations of payment service providers. **Prior to the implementation of this directive, there were no specific obligations** outlined in national legislation.

In the case of violations, Bulgaria imposes fines ranging from BGN 1,000 (over €500) to BGN 4,000 (over €2,000) for failure to declare or for false declarations. For repeated violations, the fine can increase up to BGN 10,000 (over €5,100)¹⁷¹.

3° the Member State of origin of the payment received by the beneficiary or on his behalf, the Member State of destination of the refund, as the case may be, and the information used to determine the origin of the destination of the payment or refund in accordance with Article 93duodecies/2;

4° any references that unambiguously identify the payment;

5° where applicable, information showing that the payment was initiated at the merchant's physical location.'

Art. 93duodecies/4:

'The VAT administration shall keep the information referred to in Article 93duodecies/3, in a national electronic system until 31 December of the fifth year following the year in which that information was made available in accordance with Article 93duodecies/1, § 4, 2°, in order to be able to monitor the correct application of the payment service providers' obligations and to be able to aggregate that information with other data already available to carry out targeted tax audits based on risk indicators.'

Art. 93duodecies/5:

'The King shall determine the time when the registers referred to in Article 93duodecies/1, § 4, 2°, are to be made available, as well as the detailed rules regarding the manner in which such provision is made.'

¹⁷¹ Article 192a. VAT ACT:

(1) A person who, being obliged, fails to declare or falsely declares data under Article 123 (10), or fails to declare such data within the stipulated time limits, shall be liable to a fine or a pecuniary penalty in the amount of BGN 1,000 to BGN 4,000.

Bulgaria has also **adopted the Mini One-Stop Shop (MOSS) scheme**, aligning with EU regulations to streamline VAT compliance for businesses offering cross-border digital services.

According to the national expert, to **further engage service providers in the fight against VAT fraud**, several strategies can be employed. These include:

- launching **media campaigns** for greater awareness;
- fostering **close cooperation with tax authorities**;
- offering various **incentives** to encourage service providers to report suspicious activities.

Such measures can play a crucial role in enhancing compliance and reducing VAT fraud.

Croatia

Croatia is **compliant with EU Directive 2020/284**, regarding the general obligations of payment service providers. **Prior to the implementation of this directive, there were no specific obligations** outlined in national legislation.

In the case of violations, the taxpayer is fined for a misdemeanor of 260 EUR to 66,360 EUR for failure to render available the records on payment, or for delayed declaration¹⁷².

Croatia has **adopted the MOSS Scheme**.

According to the national expert, the obligations foreseen for service providers are already enough. There is also **due diligence provisions related to money laundering**. The upgrade could be to have a **real-time reporting** to the tax administration of all transactions executed in B2B cross border transactions.

Cyprus

Cyprus **complies with EU Directive 2020/284**, which outlines the general obligations of payment service providers. Even before its implementation, **national legislation already included provisions imposing obligations on these entities**¹⁷³.

In cases of non-compliance, **penalties include a monetary fine of €20,000 and/or up to 12 months of imprisonment**.

Cyprus has **also adopted the MOSS scheme**.

According to the national expert, service providers and payment service providers should play a more active role in detecting and preventing VAT fraud-related offenses **by utilizing advanced AI**

(2) In case of a repeated violation under Paragraph (1), the fine or the pecuniary penalty shall amount from BGN 2,000 to BGN 10,000.

¹⁷² Article 131 of VAT law:

(1) A taxpayer shall be fined for a misdemeanour in the amount of EUR 260.00 to EUR 66,360.00 if:
30. fails to make available or fails to make available within the time limit laid down in Article 24b of Council Regulation (EU) No – having regard to Regulation (EC) No 904/2010 of 7 October 2010 on administrative cooperation and the fight against fraud in the field of value added tax, the records of the payee and of payments relating to the payment services provided or if fails to provide all the necessary information (Articles 83b(1) and 83d).

¹⁷³ Regulation 3(1) pursuant to Paragraph 5A of Schedule Ten.

tools to enhance fraud prevention. In Cyprus, any PSP must obtain a license from the Central Bank of Cyprus, which operates under the European Central Bank's guidance. To get licensed, PSPs must undergo a rigorous process involving extensive questionnaires, interviews, and meeting compliance requirements. This includes appointing executive and non-executive directors, a compliance officer, and an anti-money laundering officer. Compliance with European directives, particularly concerning anti-money laundering (AML) measures, is critical. The licensing process takes between one and two years, ensuring that PSPs have the necessary applications and data in place to combat digital fraud effectively. Ultimately, the license reflects the PSP's adherence to all regulatory requirements, making them better equipped to tackle cyber fraud.

Czech Republic

The Czech Republic **complies with EU Directive 2020/284**, which outlines the general obligations of payment service providers. Even before its implementation, **national legislation already included provisions imposing obligations on these entities**¹⁷⁴.

¹⁷⁴ The rules are implemented in sections 110zz to 110zzj of the VAT Act (no. 235/2004 Coll. Of Law):

§ 110zz:

Definition of basic terms

For the purposes of records on cross-border payments and their payees, the following shall be understood.

(a) a provider of a registered payment service, a person authorized under the law regulating payment transactions to provide a registered payment service, with the exception of the Czech National Bank,

(b) a registered payment service, excluding a payment service

1. enabling the deposit of cash into a payment account held by a payment service provider,

2. enabling cash withdrawal from a payment account held by a payment service provider,

3. the indirect giving of a payment order,

4. providing information about the payment account,

(c) a payment transaction under the law regulating payment transactions, if it is carried out within the framework of a registered payment service,

(d) a cross-border payment, where the State of establishment of the payer is a Member State and the State of establishment of the payee is a different Member State or a third country,

(e) a payer as defined by the law governing payment transactions,

(f) a payee as defined in accordance with the law governing payment transactions,

(g) a payment account in accordance with the law governing payment transactions,

(h) the IBAN identifier pursuant to the Regulation of the European Parliament and of the Council establishing technical and business requirements for credit transfers and direct debits in EUR,

(i) The BIC code is pursuant to the Regulation of the European Parliament and of the Council laying down technical and business requirements for credit transfers and direct debits in EUR.

§ 110zza:

State of establishment

(1) For the purposes of recording cross-border payments and their payees, the State of establishment of the payer or payee shall be the State corresponding to

(a) the IBAN identifier of the payment account of the payer or payee or any other identifier that uniquely identifies the payer or payee and their State of establishment or

(b) a BIC or other similar identifier uniquely identifying the registered payment service provider or similar provider under the law of another State acting on behalf of the payer or payee and its State of establishment, where there is no identifier under point (a).

(2) The State of establishment of a provider of a registered payment service or similar provider under the law of another State shall be, for the purposes of recording cross-border payments and their payees, the State corresponding to the BIC code or other similar identifier uniquely identifying that provider and its State of establishment.

§ 110zzb

State of provision of the service

For the purposes of recording cross-border payments and their payees, the rules governing the determination of the place of supply shall not apply to determine the State in which the recorded payment service is provided.

§ 110zzc

Obligation to keep records

(1) A provider of a registered payment service shall be obliged to keep records of cross-border payments and their payees if:

(a) provides in the domestic territory during a calendar quarter a registered payment service corresponding to more than 25 cross-border payments for the same payee and

(b) at least one of the payments referred to in point (a) meets the conditions for keeping records of cross-border payments and their payees pursuant to Section 110zdz.

(2) The number of cross-border payments for the same payee shall be determined by the individual identifiers determining the country of establishment of the payee.

(3) Where the registered payment service provider has information that a payee has several identifiers identifying his/her country of establishment, the number of cross-border payments for such payee shall be determined as the sum of all cross-border payments with these identifiers.

§ 110zdz

The scope of recording

(1) The registered payment service provider of the payee shall keep a register of cross-border payments and their payees containing information on the cross-border payment and its payee if the registered payment service corresponding to that payment is provided domestically.

(2) The registered payment service provider of the payer shall keep records of cross-border payments and their payees where the cross-border payment and its payee are not the Member State of the establishment of any registered payment service provider of the payee or of a similar provider under the legislation of another Member State.

§ 110zze

Data on cross-border payments and payees

The details of a cross-border payment and its payee shall be

(a) the BIC code or other similar identification code which uniquely identifies the provider of the payment service recorded,

(b) the name or business name of the payee as it appears in the records of the registered payment service provider,

(c) the payee's tax identification number or registration number for value added tax purposes as shown in the records of the provider of the registered payment service,

(d) the IBAN identifier or other similar identifier, if no IBAN identifier is available, which uniquely identifies the payee and his State of establishment,

(e) the BIC code or other similar identifier which uniquely identifies the registered payment service provider or similar provider under the law of another State acting on behalf of the payee and its State of establishment, where the payee receives funds without having a payment account,

(f) the address of the payee as it appears in the records of the registered payment service provider; and

(g) details of cross-border payments and details of refunds relating to those cross-border payments, namely

1. the date and time of the cross-border payment or repayment,

2. the amount and currency of the cross-border payment or repayment,

3. the Member State of origin of the cross-border payment received by or for the payee or the Member State to which the payment is returned, and the information used to determine the State of origin of the cross-border payment or the State of destination of the returned payment according to the State of establishment of the remitter,

4. other information that uniquely identifies the cross-border payment; and

5. information indicating that the initiation of the cross-border payment took place at the merchant's premises.

§ 110zzf

Obligation to provide data from records

(1) The provider of a registered payment service shall submit a notification containing data from the register on cross-border payments and their recipients to the tax administrator by the end of the calendar month immediately following the end of the calendar quarter to which the data relate.

(2) Where the last day of the deadline referred to in paragraph (1) falls on a Saturday, Sunday, or public holiday, the deadline shall be that day.

(3) If the provider of a registered payment service discovers that it has provided incorrect or incomplete data in the notification under paragraph (1), it shall, within 5 working days from the date of discovery of the

Failure to comply with non-monetary tax obligations under § 247a of the Tax Procedure Code can result in **fin**es of up to 500,000 CZK (approximately 20,000 EUR). This applies to individuals who fail to meet registration, reporting, or record-keeping requirements. Additionally, failure to correct filing defects upon notice from the tax administrator incurs a penalty of 1,000 CZK (approximately 40 EUR), which can be increased to 50,000 CZK (approximately 2,000 EUR) if it significantly hinders tax administration. **Fines must be paid within 30 days of notification, and penalties can be imposed within three years of the violation.**

The Czech Republic **has adopted the MOSS Scheme.**

According to the national expert, **platforms** (especially those facilitating accommodation and personal transport) **should pay VAT on behalf of small suppliers or suppliers not established in the EU who use their platform for the provision of their services. Platforms should act as a deemed supplier of services purchased through their webpage. They should also provide data on all transactions to tax administrations.**

Denmark

Denmark **is compliant with EU Directive 2020/284**, regarding the general obligations of payment service providers. **Prior to the implementation of this directive, there were no specific obligations outlined in national legislation.**

There are **no specific sanctions for breaches of obligations by payment service providers (PSPs); only the penalties outlined in the VAT Code apply.**

Denmark **has adopted the MOSS Scheme.**

According to the national expert, **digital reporting** would help to further engage the PSPs in the fight against VAT fraud.

incorrect or incomplete data, submit a subsequent notification to the tax administrator in which it shall correct the deficiencies.

§ 110zzg

Keeping data and obligation to provide data from the register on request

The registered payment service provider shall be obliged to keep the data from the register on cross-border payments and their recipients electronically for 3 years from the end of the calendar year in which the cross-border payment was made; the registered payment service provider shall be obliged to submit a notification containing such data to the tax administrator upon his request.

§ 110zzh

Method of submitting the notification

(1) Notifications pursuant to sections 110zzf and 110zzg shall be submitted in a form electronically through the public administration information system administered for this purpose by the Tax Administration authority of the Czech Republic.

(2) A notification made in a manner other than pursuant to subsection (1) shall be ineffective. If the notification is submitted by means of a data message requiring additional confirmation, it shall be confirmed under the conditions specified in the Tax Code within the time limit for submission of the notification.

§ Section 110zzi

Status of the registered payment service provider

The registered payment service provider shall have the status of a taxable subject for the purposes of the records on cross-border payments and their payees.

§ 110zzi

Tax administrator

In the case of records of cross-border payments and their payees, the Specialised Tax Office shall be the tax administrator.

Estonia

Estonia **has implemented the Council Directive (EU) 2020/284**, which introduces new record-keeping and reporting obligations for payment service providers (PSPs) to combat VAT fraud in cross-border e-commerce. Effective from January 1, 2024, Estonian PSPs are required to collect and report information on cross-border payments to the Estonian Tax and Customs Board, which then transmits this data to the Central Electronic System of Payment Information (CESOP). This initiative aims to enhance the detection of potential e-commerce VAT fraud by monitoring cross-border transactions.

Estonia has also adopted the **Mini One Stop Shop (MOSS) Scheme** and its **extension OSS Scheme**.

Finland

Finland is compliant with **EU Directive 2020/284**, which establishes general obligations for payment service providers (PSPs). Even before its implementation, Finnish national legislation already imposed certain obligations on these entities, **though not to the same extent as the Directive¹⁷⁵. In case of breach, fines** between €2,000 and €15,000 are foreseen [Article 22a¹⁷⁶]. **Finland has adopted the MOSS Scheme.**

¹⁷⁵ Article 29.7:

The tax administration can issue more detailed regulations on the information to be provided, the time and method of providing the information, and limit the obligation to provide information in situations that are of minor financial or tax supervisory importance.

¹⁷⁶ Article 22a:

Negligence Penalty (§ 247a Tax Procedure Code)

A negligence penalty of up to €2,000 may be imposed on an entity required to provide information if:

1. There is a minor deficiency or error in the submitted declaration, information, document, or procedure required to fulfill the obligation, and the entity has not corrected it despite receiving a formal notice.
2. The entity delays submission of the required declaration, information, or document without a valid reason.
3. The information is provided in a manner not compliant with legal requirements or contrary to the tax authority's instructions.

If the submitted declaration, information, or document is significantly incomplete or incorrect, or if it is provided only after receiving a formal request, a higher penalty of up to €5,000 may be imposed.

In cases of intentional or grossly negligent non-compliance, such as submitting substantially false information or failing to fulfill an obligation entirely or significantly, the penalty can be up to €15,000.

Additional Considerations:

- The penalty amount considers the scope of the required information.
- The penalty is imposed in full hundreds of euros.
- If the main contractor or general developer fails to provide accurate information due to the negligence of an employer or independent contractor, no penalty is imposed if the tax authority is notified of the failure.
- Natural persons and estates are exempt from penalties unless the negligence concerns business, agriculture, or forestry activities. However, a penalty may still apply to representatives under the Posting of Workers Act or private developers who fail to comply with reporting obligations.
- The penalty is not tax-deductible and is remitted to the state.
- Interest is charged on unpaid penalties as per the law on tax surcharges and late-payment interest.

France

According to the national expert, France is not compliant with Directive 2020/284, and the transposition is not in progress.

In addition, there are **no specific provisions assigning responsibility or obligations to payment service providers (PSPs) under French national law**. However, **platforms deemed non-compliant due to repeated tax violations may be included in a "grey list"** as per Article 1740 D of the General Tax Code (CGI)¹⁷⁷. This measure aims to identify and monitor entities that consistently fail to meet tax obligations, thereby enhancing transparency and compliance within the digital economy.

France **had adopted the MOSS Scheme and its extension OSS Scheme**.

Finally, according to the national expert, French service providers and payment service providers can play a significant role in detecting and preventing VAT fraud by **adopting a proactive and collaborative approach**, implementing robust security measures and collaborating closely with competent authorities, such as:

- Implementing transaction monitoring systems.
- Centralized alerts and suspicious transaction detection.
- Data sharing between providers, bans and regulators.
- Use data analysis and artificial intelligence techniques to examine large volumes of transaction data and identify anomalies that may indicate possible VAT fraud.
- Sharing relevant information and suspicious transaction reports to assist with VAT fraud investigations and enforcement.
- They can strengthen their internal controls and due diligence procedures, etc.

Germany

Germany **complies with EU Directive 2020/284**, which outlines the general obligations of payment service providers. Even before its implementation, **national legislation already included provisions imposing obligations on these entities**¹⁷⁸.

In **case of breach**, fines up to €5,000 are foreseen¹⁷⁹.

-
- If a late fee is imposed under the Income Information System Act, an additional negligence penalty under this section will not be imposed for the same delay.

¹⁷⁷ Article 1740 D of the General Tax Code:

The list of platform operators deemed non-cooperative due to repeated non-compliance with their tax obligations in France may be published on the tax administration's website for a period not exceeding one year or until full payment of the associated taxes and penalties is made.

¹⁷⁸ § 22 g VAT Act

Introduced by Art. 10 of the Annual Tax Act 2022 Federal Law Gazette I 2022, 229.

¹⁷⁹ Under Germany's Value Added Tax Act (UStG), Section 26a outlines administrative offenses related to VAT compliance. Violations include failing to timely or fully remit advance payments, differences, or assessed taxes; issuing invoices late or not at all; inadequate record-keeping; and failing to submit required reports. Penalties for such offenses can reach up to €30,000, depending on the severity and nature of the violation.

Germany has adopted the MOSS Scheme.

According to the national expert, it would be worth considering introducing obligations similar to those for combating money laundering or making better use of the data obtained from the money laundering reporting obligation. Typically, the same risk criteria are used in both areas to indicate illegal activities.

Greece

Article 15D of the Greek Code of Tax Procedures introduces obligations for payment service providers (PSPs) to combat Value Added Tax (VAT) fraud. This article was incorporated through Article 5 of Law 5073/2023, which aligns Greek legislation with Council Directive (EU) 2020/284 of 18 February 2020. Previously, there were no specific provisions regarding this matter.

Sanctions for PSPs failing to meet the obligations outlined in Article 15D are specified in Article 54ID of the same Code¹⁸⁰. These penalties aim to enforce compliance and deter non-compliance among PSPs operating within Greece's tax framework.

Greece has adopted the MOSS Scheme.

Finally, according to the national expert, payment services providers should be more involved in the detection and prevention of criminal offenses related to VAT fraud. Payment services providers should adopt a risk-based approach to identify VAT fraud risks.

¹⁸⁰ Article 54ID of Code of Tax Procedure:

1. Payment service providers who violate Article 15D shall be fined if:

- a) they submit the records of par. 2 of article 15D after the deadline,
- b) they do not submit the records of par. 2 of article 15D,
- c) submit incomplete or inaccurate records of par. 2 of article 15D,
- d) do not respond to a request from the Tax Administration for the provision of information or for the completion or correction of information or data referred to in article 15D, within the set deadline,
- e) do not cooperate during an audit for compliance with the data submission rules,
- f) do not comply with the obligations of payment service providers, regarding beneficiaries and payments, in accordance with paragraphs 2, 3 and 4 of article 15D.

2. The fines for the violations of paragraph 1 are determined as follows:

- a) one hundred (100) euros, for each violation of case a' , per beneficiary,
- b) three hundred (300) euros, for each violation of cases b' and c' , per beneficiary,
- c) one thousand (1,000) euros, for each violation of case d' , per beneficiary,
- d) two thousand five hundred (2,500) euros, for each violation of case e' ,
- e) five thousand (5,000) euros, for each violation of case f' .

The total amount of fines imposed per compliance check for violation of the obligations of Article 15D cannot exceed the amount of five hundred thousand (500,000) euros.

For the violations of case a' of paragraph 1, the total amount of fines, per reference year, cannot exceed the amount of ten thousand (10,000) euros.

3. If the payment service providers commit the same violation, within five years of the finding of the initial violation, the fines of par. 2 shall be doubled. In the event of the same violation being committed again for the third or more times, four times the initial fine shall be imposed, regardless of the time it was committed, subject to the second and third paragraphs of par. 2".

Hungary

Hungary **complies with Directive 2020/284** concerning the obligations of payment service providers (PSPs). Prior to its transposition, certain provisions addressed PSP obligations, notably Articles 183/B to 183/E of the Hungarian VAT Act.

Following the Directive's implementation, the Act on the Rules of Taxation has been amended to enhance compliance measures. Effective from 1 August 2024, the default penalty amounts have been increased, up to HUF 5 million (approximately EUR 12'500) [Article 229/A of the Act CL of 2017¹⁸¹].

Hungary has adopted the MOSS Scheme.

According to the national expert, **besides the reporting obligation, a VAT withholding mechanism could also be introduced** (LATAM example) to involve in further way PSPs in the detection and prevention of criminal offenses related to VAT fraud, however, this might be too burdensome on the sector.

Ireland

Ireland **is compliant with Directive 2020/284**. This was transposed via S.I. No. 650/2023 – European Union (Value-Added Tax) Regulations 2023. It is important to notice that there was an issue of failure to transpose earlier in 2024¹⁸². **Prior to the implementation of this directive, there were no specific obligations** outlined in national legislation.

There are **no additional sanctions for this new legislation but the usual tax penalties would apply**.

The Irish expert explained that the Revenue Commissioners are experienced professionals with extensive knowledge of corporate matters and the relevant legislation. It is possible that the prosecutor may lack the institutional knowledge required to process this type of crime. In contrast, the revenue authority possesses extensive experience in this domain. Furthermore, the criminal law system is less experienced in prosecuting economic crimes, which are inherently more complex than “conventional” crimes such as assault. This distinction between traditional and non-traditional crimes allows for a division of labor between the revenue authorities and the police and prosecution services. The former are responsible for addressing revenue offenses through their administrative process, while the latter handle more conventional criminal activities. In Ireland, approximately twice a year, the Revenue Commissioners publish a list of individuals who have not paid the requisite tax amount (approximately €12,000-€13,000). This list is disseminated through various print media outlets. This practice is indicative of the fact that the administrative authority,

¹⁸¹ Article 229/A of the Act CL of 2017:

"(1) Failure to comply with the record-keeping obligation pursuant to Section 183/C (1) of the VAT Act, late, incorrect or incomplete compliance with the obligation to provide information pursuant to Section 183/C (2) of the VAT Act, and failure to comply with the obligation to provide information pursuant to Section 183/C (2) of the VAT Act, or late, incorrect or incomplete compliance with the obligation to provide information pursuant to Section 183/C (2) of the VAT Act. 183/C (7), the state tax and customs authority may impose a default fine of up to HUF 5 million on the person obliged to keep records, provide data and keep records. (2) No default fine shall be imposed under paragraph (1) if the person required to keep, provide and preserve records excuses his default, delay, defective or incomplete performance by proving that he acted as is normally expected in the given situation."

¹⁸² Regarding an error in the notification sent to the Commission via the Themis system and failure to include a correlation table and explanatory letter. This was rectified as of 29 February 2024.

in this case, also serves a shaming function. The publication of names in this manner serves to fulfill the shaming function that is sometimes expected from criminal law.

Finally, the expert underlined that sometimes the problem is the overuse of criminal law, in terms of over-criminalisation.

Ireland introduced, but has since removed, the MOSS scheme. MOSS was applicable in Ireland but was discontinued as of 1st July 2021. Services previously covered under MOSS are **now covered by the One Stop Shop (OSS).**

According to the national expert, perhaps **further efforts in respect of reporting of suspicious transactions or activities could aid the detection and prevention of VAT fraud.** Firstly, encouraging greater use of such processes (even where not necessarily required to do so) could add to the information available to enforcement bodies in Ireland. Secondly, perhaps such payment service providers **could provide more analysis and reporting regarding the suspicious transactions and activities observed** (e.g. identifying trends, and consolidating findings). In Ireland it is the Central Bank that oversees and monitors Payment Service Providers (PSPs).

Large financial institutions have the capacity to handle reporting and compliance obligations because they are very familiar with the money laundering obligations that are imposed on banks and other institutions, and they simply have divisions within their companies to handle anti-money laundering.

Italy

Italy is compliant with Directive 2020/284. The transposition took place with Legislative Decree 153/2023. Prior to the implementation of this directive, there were no specific obligations outlined in national legislation.

Article 2 of the Legislative Decree 253/2023 establishes **the following sanctions for non-compliance with VAT obligations:**

- **Failure to Retain Records:** Violations of record-keeping obligations are subject to administrative fines ranging from €1,000 to €8,000, as outlined in Article 9, paragraph 1, of Legislative Decree No. 471/1997 [Article 40-ter].
- **Failure to Submit Reports:** Violations of reporting obligations incur administrative fines between €1,500 and €15,000, in accordance with Article 10, paragraph 1, of Legislative Decree No. 471/1997. The fine is reduced by half if the report is submitted within fifteen days after the due date. [Article 40-quarter].

Italy has adopted the MOSS Scheme and its extension the OSS Scheme.

According to the national expert, **the mechanism of administrative sanctions is more efficient**, its set of legal obligations could be understood as a duty to act on these service providers, and therefore there could be a risk of using this type of legal obligation to hold them responsible for a failure to prevent crime. It is more proportionate and also gives more guarantees to companies, because the administrative penalties, if added together, are very severe and also lead to shameful consequences, as the experts said earlier. **The most crucial aspect from their perspective is the accessibility of the data collected by the service providers to the administrative authority.** This can be achieved by facilitating direct access to the data, for instance through a unified database that is directly accessible by the police.

Latvia

Latvia complies with Directive 2020/284 concerning the obligations of payment service providers (PSPs). Prior to its transposition, certain provisions addressed PSP obligations, notably Section 147 and 148 of Latvia's Value Added Tax (VAT) Act¹⁸³.

For the failure to provide information, inadequate provision of information, or provision of false information to the State Revenue Service, a warning or a fine of up to EUR 700 shall be imposed on a natural person or a board member with or without deprivation of the board member's right to hold specific offices in commercial companies for a period up to three years [Section 3, para 2, Law on Administrative Penalties for Offences in the Field of Administration, Public Order, and Use of the Official Language].

¹⁸³ Section 147 Latvia's Value Added Tax (VAT) Act:

Obligation to Maintain Records, Retain, and Provide Information on Payment Recipients and Cross-Border Payments to Prevent Tax Evasion in Cross-Border Transactions

1. For the purposes of this section:

- a) Payment Service Provider refers to an entity specified in Section 2, Paragraph 2, Clauses 1, 2, 4, 7, or 8 of the Law on Payment Services and Electronic Money.
- b) Payment Service denotes a service outlined in Section 1, Paragraph 1, Subclauses (c), (d), (e), or (f) of the aforementioned Law.
- c) Payer is a natural or legal person defined in Section 1, Paragraph 5 of the Law on Payment Services and Electronic Money.
- d) Payment Recipient is a natural or legal person defined in Section 1, Paragraph 6 of the same Law.
- e) Cross-Border Payment is a payment as described in Section 1, Paragraphs 3 or 9 of the Law on Payment Services and Electronic Money, considering the exceptions in Section 3 of that Law, where the payer resides in one Member State and the payment recipient resides in another Member State, third country, or territory.

2. Payment Service Providers are required to:

- a) Maintain detailed records of payment recipients and cross-border payments for each calendar quarter, specifically for those services provided in that quarter to a single payment recipient, if they exceed 25 cross-border payments.
- b) Submit the information specified in this section regarding payment recipients and cross-border payments to the State Revenue Service.
- c) Retain identification data of payment recipients and details of cross-border payments in electronic format for three calendar years, starting from the end of the calendar year in which the payment was made.

3. If a Payment Service Provider offers payment services in a participating Member State other than Latvia, they are not obligated to provide the State Revenue Service with the information specified in this section regarding payment recipients and cross-border payments.

4. The obligations outlined in Paragraph 2 of this section do not apply to payment services where at least one of the payment recipient's service providers is located in another Member State. However, the payer's Payment Service Provider must include such payments in the count of cross-border payments.

5. The Cabinet of Ministers shall determine:

- a) The identification data of legal and natural persons and cross-border payment details to be submitted to the State Revenue Service.
- b) The methodology for calculating the number of cross-border payments by Payment Service Providers.
- c) The procedures for obtaining, verifying, and submitting information to the State Revenue Service.
- d) The manner in which the State Revenue Service processes the information provided in the Centralized Electronic Payment Information System.

Article 148:

Data Protection in the Exchange of Information on Payment Recipients and Cross-Border Payments

- 1. The State Revenue Service is the controller of data provided to the Centralized Electronic Payment Information System.
- 2. To ensure the transmission of information about payment recipients and cross-border payments to the Centralized Electronic Payment Information System, both payment service providers and the State Revenue Service process personal identification data and data concerning cross-border payments.

Latvia has adopted the MOSS Scheme.

According to the national expert, payment service providers and other service entities could play a more integral role in the detection and prevention of VAT fraud **by being formally designated as obliged entities under the law**. This would entail a legal obligation for these providers to monitor, report, and cooperate with authorities regarding suspicious transactions that may indicate fraudulent activity. By enhancing their role within the regulatory framework, these entities could significantly contribute to the early detection of VAT fraud and strengthen the overall preventive measures.

Lithuania

Lithuania **complies with EU Directive 2020/284**, which outlines the general obligations of payment service providers. Even before its implementation, **national legislation already included provisions imposing obligations on these entities**¹⁸⁴.

The Code of administrative offences provides administrative liability in cases where the payment service provider did not comply with the recording/reporting obligations in Lithuania¹⁸⁵.

Lithuania **has adopted the MOSS Scheme**. Moreover, Lithuania **also implemented the One Stop Shop (OSS)** system in 2021. This system is designed to lighten the VAT burden for the businesses engaged in the supply of electronic and other services (whose place of supply is in other EU member states) and make distance sales of goods to non-taxable persons in cases where the supply takes place in more than one EU member state.

According to the national expert, **administrative liability for legal persons is more efficient**, especially from the point of view of procedure: criminal procedure takes a lot of time and effort. In the opinion of the majority of experts, currently the Lithuanian legal system provides enough obligations, as well as rights, which, if used, would make service providers and payment service providers more involved in the detection and prevention of criminal offenses related to VAT and cyber VAT fraud. For, example, according to the Law on Prevention of Money Laundering and Terrorist Financing, some service providers and all payment service providers must provide, *inter alia*, information on suspicious and other identified monetary transactions to the Financial Crimes Investigation Service. Moreover, it should be noted that the Law on Protection of Whistleblowers has been in force in Lithuania since January 1, 2019, which provides for the following main measures to protect, encourage and support persons (including service providers and payment service providers) who have provided information on breaches: 1) securing safe channels for providing information on breaches; 2) ensuring a person's confidentiality; 3) prohibition from adversely affecting a person who has provided information on breaches; 4) right to remuneration

¹⁸⁴ Laws No. XIV-1659 and No. IX-2112 amending Law on Tax Administration. TAR, 2022-12-22, No. 2022-26363.

¹⁸⁵ Article 188:

Non-compliance with the requirements set for payment service providers

1. Non-compliance with the requirements set forth in the Tax Administration Law of Republic of Lithuania and its implementing legal acts for payment service providers,

imposes fine on managers of legal entity or other responsible persons from 1 800 to 3 800 euros.

2. The administrative offence provided for in paragraph 1 of this Article, committed repeatedly, imposes fine on managers of legal entity or other responsible persons from 3 800 to 6 000 euros.

for valuable information; 5) right to compensation; 6) ensuring free legal aid; 7) exemption from liability.

For this reason, is **currently more important to assess the effectiveness of the application of the mentioned laws** (especially the Law on Protection of Whistleblowers) **and to identify the strengths and weaknesses of national legal regulation.**

Luxembourg

Luxembourg is compliant with Directive 2020/284. Prior to the implementation of this directive, there were no specific obligations outlined in national legislation.

In the event of **breaches**, Luxembourg's legislation stipulates **standard fines and sanctions**. According to Article 77 of the Luxembourg VAT law, **administrative fines** can be imposed for various infringements. For instance, intentional inaccuracies in tax returns can lead to fines ranging from 5% to 25% of the evaded taxes. Simple tax fraud carries fines between 10% and 50% of the evaded taxes, while involuntary tax fraud results in fines from 5% to 25% of the evaded taxes. Additionally, aggravated tax fraud and tax fraud are criminal offenses **punishable by imprisonment and substantial fines**, depending on the severity of the offense.

Luxembourg has applied the MOSS Scheme.

National experts and EU Commission assessments indicate that **the reporting obligations imposed on Payment Service Providers (PSPs), alongside those of goods and services providers (such as EC sales lists and MOSS), are designed to enhance the early detection and prevention of VAT fraud.** The effectiveness of these measures will become evident once PSPs submit their initial reports by April 30. However, due to technical challenges in reporting across certain countries and the complexities PSPs face in accurately identifying reportable transactions, the initial reporting periods may yield limited insights.

Malta

Malta **complies with EU Directive 2020/284**, which outlines the general obligations of payment service providers. Even before its implementation, **national legislation already included provisions imposing obligations on these entities.**

Article 11 of Legislative Decree No. 272 of 2023, which transposes the EU directive, stipulates that payment service providers (PSPs) failing to submit required information within specified deadlines are subject to **administrative penalties** as outlined in Article 38(2)(c) of the VAT Act. Additionally, if a PSP does not comply with regulatory requirements after receiving two electronic reminders over a three-month period, or submits misleading or false information, senior managing officials of the PSP may face fines ranging from €10,000 to €30,000 per offense. Non-compliance may also result in daily fines of €50 until the issue is rectified¹⁸⁶.

¹⁸⁶ Article 77 of the VAT Code:

“77. Any person who –

(p) being a credit or financial institution which supplies money or grants credit by way of a loan account facility or by means of any other kind of facility to a customer in connection with the supply of goods or services by third parties to that customer for the construction, re-construction, repair, refurbishment or maintenance of immovable property or for fixtures related thereto, and which effects payment for such goods

Malta has adopted the MOSS Scheme.

According to the national expert, in Malta, Service Providers are already overwhelmed with existing reporting obligations. **Adding further reporting obligations would create an excessive burden.**

The Netherlands

The Netherlands **has implemented Directive 2020/284** concerning obligations for payment service providers (PSPs). **Prior to this transposition, Dutch legislation did not include specific obligations in this area.**

Article 41 of the Netherlands' Act on Turnover Tax 1968 stipulates that in the event of a breach, an **administrative fine** from the sixth category may be imposed, amounting to up to 10% of the company's turnover from the previous year¹⁸⁷.

The Netherlands has adopted the MOSS Scheme.

The Netherlands' expert highlights that, according to Directive 2020/284, payment service providers are required to provide their tax authorities with information on the payments made through their systems in accordance with Regulation 904/2010 (Art 243b(4)(b)). That Regulation

or services either directly to the vendor or supplier thereof or to a third party or to the customer subject to an understanding or to an express or implied condition that the amount paid will be passed on to the said vendor or supplier, by the debit of the customer's loan account or other facility, on the basis of supporting documents, including contracts, invoices, receipts, architects' or other certificates, or similar documents, submitted by or on behalf of the customer or by or on behalf of suppliers, contractors or other third parties, and which fails to inform the Commissioner of the names and VAT registration numbers of the said suppliers, contractors or other third parties as aforesaid, other than the customer, to whom it has directly or indirectly made payments as specified in this paragraph, in the form required by the Commissioner, as well as of the amounts of such payments, by not later than the end of the calendar quarter immediately following the calendar quarter during which it directly or indirectly made any payment as aforesaid, shall be guilty of an offence and shall, on conviction, be liable -

(i) to a fine of not less than six thousand euro (€6,000) and not exceeding ten thousand euro (€10,000) for an offence committed under paragraphs (c) and (d); and

(ii) to a fine of not less than seven hundred euro (€700) and not exceeding three thousand five hundred euro (€3,500) for an offence under the other paragraphs, and in addition, for any offence as above referred to in all paragraphs, except for paragraph (p), where tax amounting to more than one hundred euro (€100) would be endangered, to a further fine equal to two times the endangered tax or to imprisonment of not more than six months or to both such fines and imprisonment:

Provided that, the two times fine for the endangered tax shall in no case be less than one thousand euro (€1,000).

In addition, on a request by the prosecution, the court shall order the offender to comply with the law within a time sufficient for the purpose, but in any case not exceeding one month, and, in default, the offender shall be liable to the payment of a further fine of five euro (€5) for every day on which the default continues after the lapse of the time fixed by the Court."

¹⁸⁷ Act on Turnover Tax 1968 - Article 41:

1. If failure to comply with the obligations referred to in Chapter VI, Section 6 is due to intent or gross negligence on the part of the payment service provider, this constitutes an offense for which the inspector shall impose an administrative fine on him not exceeding amount of the sixth category, referred to in Article 23, fourth paragraph of the Criminal Code.

2. The first paragraph applies mutatis mutandis if a payment service provider provides payment data to the Tax Authorities that relate to fewer than 26 cross-border payments to the same beneficiary in the course of a calendar quarter.

3. The authority to impose the fine referred to in the first paragraph shall lapse, notwithstanding Article 5:45, second paragraph of the General Administrative Law Act, after five years after the end of the calendar year in which the activities referred to in Chapter VI, section 6 obligations have arisen.

leaves the choice to member states whether they collect the information once every three months, within one month after the quarter ends, or by means of an electronic standard form (Art. 24b(1)). **It would be preferable to introduce an obligatory system comparable to the system of e-invoicing, which automatically and almost in real-time informs the tax authorities of all financial transactions made through the payment services provider.** In that way, the tax authorities would be in a much better position to quickly intervene and act on a suspicion of VAT fraud.

Poland

Poland has **fully implemented Directive 2020/284**, which introduces new reporting obligations for payment service providers (PSPs) to combat VAT fraud. **Prior to this transposition, Polish legislation already imposed specific obligations on PSPs.** The new requirements, effective from 1 January 2024, mandate that PSPs maintain records of cross-border payments and report certain transactions to the Central Electronic System of Payment Information (CESOP). This initiative aligns with the European Union's efforts to enhance administrative cooperation and address VAT fraud in cross-border e-commerce.

The National e-Invoice System (KSeF) is a solution enabling the issuance and sharing of structured electronic VAT invoices. The basic idea was to introduce this solution in two stages. In the initial period, structured electronic invoices were supposed to function as an optional solution. From October to December 2021, a special pilotage – testing period of this solution was conducted with the participation of taxpayers. After its completion, from January 1, 2022, by the Act of October 29, 2021, amending the Act on tax on goods and services and certain other acts (Journal of Laws of 2021, item 2076), the National e-Invoice System was introduced as a voluntary solution. From that moment, it became possible to issue structured electronic invoices within the National e-invoice System (KSeF). At the same time, work was undertaken to introduce mandatory electronic invoicing. The Council of the European Union agreed to this by derogation decision number 2022/1003 of June 17, 2022. Based on this, it was planned to introduce mandatory electronic invoicing from July 2024. However, on June 10, 2024, an amendment to the VAT Act was published (Act of May 9, 2024, amending the Act on tax on goods and services and certain other acts (Journal of Laws of 2024, item 852), which postpones the obligation to issue e-invoices to February 1, 2026. This means that until then, the rules for issuing electronic invoices remain unchanged, issuing structured invoices within the National e-Invoice System (KSeF) is possible but not obligatory

In the event of a breach of the rules of conducting business as a VAT payer, it is possible to remove it from the VAT register. Data of VAT payers are collected in the VAT payer register. The Head of the National Tax Administration keeps an electronic list of VAT subjects that have not been registered by the head of the tax office or that have been removed from the register as VAT payers by the head of the tax office, registered as VAT payers, including subjects whose registration as VAT payers has been restored. Subjects can be checked in the list as of a selected date, falling no earlier than in the period of 5 years preceding the year in which the entity is checked. The list includes, among others: numbers of settlement accounts or registered accounts in the cooperative savings and credit union of which the entity is a member: opened in connection with his business activity and indicated in the identification application or update notification and confirmed using the special STIR electronic system¹⁸⁸.

¹⁸⁸ Art. 96b goods and services tax act:

According to the national expert, Poland **has not applied the MOSS Scheme**.

The expert highlights that in Poland, **administrative tools are employed**, albeit with considerable rigidity. This is due to the presence of internal legislation that empowers the tax authority to automatically block transactions within the financial system in instances of suspected fraud. The duration of such blocks may extend to either 72 hours or three months. The proportionality of this system is a subject of ongoing debate in Poland.

Portugal

Portugal **complies with Directive 2020/284**, which was **transposed** into national law through **Law No. 81/2023**, published on December 28, 2023, and effective from January 1, 2024. This law imposes obligations on payment service providers (PSPs) to maintain electronic records of cross-

1. The Head of the Domestic Fiscal Administration shall keep the lists of the following subjects in electronic form:

1) as regards which the head of a revenue office did not make a registration or which the head of the revenue office removed from the register as VAT payers.

2) registered as VAT payers, including the subjects, the registration of which as VAT payers has been restored.

2. The list is made available in the Biuletyn Informacji Publicznej [Public Information Bulletin] on a dedicated website of the office providing support to the minister competent for public finance in such a manner as to enable to verify whether the subject is contained in the list as at a selected date falling not earlier than within 5 years preceding the year in which the subject is subject to verification. The data of this subject shall be made available pursuant to the condition as at the selected date, excluding the data made available pursuant to the condition as at the day of making the verification.

3. the list shall include the following data of the subjects referred to in paragraph 1:

1) the name (business name) or forename and surname.

2) the number by means of which the taxpayer has been identified for tax purposes, provided that such a number has been assigned.

2a) the status of the subject:

a) as regards which the registration was not made, or which has been removed from the register as a VAT payer.

b) registered as an "active VAT payer" or an "exempt VAT payer", including the subject, the registration of which has been restored.

3) the REGON identification number, if one has been assigned.

4) repealed.

5) the number in the National Court Register, if one has been assigned.

6) the address of the seat – in the case of a subject other than a natural person.

7) the address of the permanent place of pursuit of activity or the place of residence address in the case of the lack of the permanent place of pursuit of activity – with regard to a natural person.

8) the forenames and surnames of persons being members of the body authorized to represent the subject and their tax identification numbers.

9) the forenames and surnames of procurators and their tax identification numbers.

10) the forename and surname or business name (name) of the shareholder and his tax identification number.

11) the dates of registration, refusals of registration or striking off the register and restoring the registration as a VAT payer.

12) the legal grounds for refusals of registration or striking off the register and restoring the registration as a VAT payer, respectively.

13) the numbers of settlement accounts referred to in Article 49, paragraph 1, subparagraph 1 of the Act of 29 August 1997 – Banking Law, or personal accounts in a cooperative savings and credit fund, of which the subject is a member, opened in connection with the economic activity conducted by the member:

a) such settlement accounts being indicated in a notification of identification particulars or notification of updating particulars and

b) confirmed with the use of the STIR within the meaning of Article 119zg, subparagraph 6 of the Tax Ordinance, except for the accounts maintained by the National Bank of Poland.

border payments and their beneficiaries for three years. Specifically, PSPs executing more than 25 cross-border payments to the same payee within a quarter are required to report this information quarterly to the Tax and Customs Authority (AT). The reporting is done using standardized electronic forms, as defined by Portaria No. 81/2024/1, published on March 5, 2024. **Prior to this legislation, there were no provisions requiring PSPs to report such data. Non-compliance with these obligations can result in administrative fines**, as outlined in Articles 117 and 119-B of Law No. 15/2001.

Portugal has adopted the MOSS Scheme.

In order to involved in further way the PSPs on the fight against VAT fraud, the national expert suggested a first **consensual approach, leaving the punitive response for a later stage**, in accordance with the teachings of John Braithwaite, an Australian criminologist who served as a supervisor at the Australian tax authority and has published several studies on this subject.

Romania

Romania **has fully complied with Directive 2020/284**. Prior to its transposition, Romanian national legislation **did not impose specific recording or reporting obligations on payment service providers (PSPs)**.

Article 59 of the Tax Procedure Code outlines the general obligation of taxpayers to provide information to the tax authority:

- **Periodic Reporting:** Taxpayers must periodically furnish the central tax authority with information regarding their activities.
- **Reporting by Electronic Interface Providers:** Taxpayers offering electronic interfaces facilitating online business transactions are required to report information on transactions conducted through these platforms.
- **Data Submission:** The information is submitted based on a declaration issued by the taxpayer.
- **Regulatory Details:** The specifics regarding the nature of the information, reporting frequency, and declaration formats are approved by an order from the President of the National Agency for Fiscal Administration (NAFA).

Following the adoption of Government Emergency Ordinance No. 67/2022, additional amendments were made to Article 59:

- **Postal Service Providers' Reporting Obligations:** Postal service providers delivering items with cash-on-delivery features must monthly report specific data to the central tax authority.
- **Information to be Reported:** Details include registration number, mailing date, sender's identification, recipient's name, shipping and delivery addresses, and the value of the delivered goods.
- **Data Retention:** The reported data must be stored for five years from receipt by the tax authority, after which they are automatically deleted.
- **Data Subject Rights:** Individuals whose data are processed have rights as per Regulation (EU) 2016/679 on data protection.

To implement these provisions, NAFA's President issued Order No. 1644/2022, which:

- **Approves the Model and Content:** Sets the format for the informative declaration regarding cash-on-delivery postal items.
- **Details Submission Procedures:** Provides instructions on completing and submitting the declaration.
- **Regulates Data Handling:** Ensures personal data processing aligns with data protection regulations.

This order came into force upon publication, with reporting obligations for postal service providers commencing on January 30, 2023.

According to NAFA's semiannual report, in June 2023, the tax authority issued 2,851 notifications to individuals who received funds via postal service providers, totaling RON 475.02 million. These notifications reminded recipients of their obligation to submit income tax returns by May 25 of the following year.

Regarding **sanctions for non-compliance**, the new law does not specify particular penalties for PSPs failing to meet the CESOP reporting obligations. Instead, such failures fall under the **general provisions of the Tax Procedure Code**. Article 336 of the Code stipulates **fin**es for taxpayers who do not submit required information to tax authorities within established deadlines. The fines range from RON 1,000 (approximately 200 EUR) to RON 5,000 for medium and large taxpayers, and from RON 500 (approximately 20 EUR) to RON 1,000 for other taxpayers.

Additionally, Law No. 126/2024 introduces stricter penalties for acts of tax evasion, including **criminalization of certain offenses** and increased prison sentences.

Romania **has adopted the MOSS Scheme and its extension OSS Scheme**. The national expert declared that the OSS is more efficient than the MOSS scheme but both are a step forward in the collection of VAT, which also reduces the burden on taxpayers. It would be better to have them mandatory and not optional.

Finally, according to the national expert, while Romania has established **robust reporting requirements for PSPs**, ongoing efforts are necessary to **bolster the tax authority's capacity to effectively interpret and utilize the information provided**. Continued investment in **training, system enhancements, and international collaboration** will be crucial to fully harness the potential of these data in combating tax fraud.

Slovakia

Slovakia is **fully compliant with Directive 2020/284**. Even before the implementation, the national legislation foreseen obligation for the PSPs¹⁸⁹.

¹⁸⁹ Law no. 222/2004 Coll. of the Value Added Tax Act - § 70a:

Payment service providers

(1) For the purposes of this provision

a) the provider of payment services is the provider of payment services according to a special regulation, 28h)

b) a domestic payment service provider is a payment service provider according to letter a), whose home Member State or host Member State is the country,

c) a payment service is a payment service according to a special regulation, 28i)

-
- d) payment is a payment operation^{28j)} or money transfer^{28k)}
- e) the payment provider is the payer according to a special regulation, ^{28l)}
- f) the recipient of the payment is the recipient, ^{28m)}
- g) the home Member State is the home Member State according to a special regulation, ²⁸ⁿ⁾
- h) the host member state is the host member state according to a special regulation, ^{28o)}
- i) a cross-border payment is a payment if the payment provider is located in a member state determined pursuant to paragraph 6 and the recipient of the payment is located in another member state or in a third country determined pursuant to paragraph 7.
- (2) The domestic payment service provider is obliged, for the purpose of carrying out control of the delivery of goods or the delivery of a service with a place of delivery in the territory of the European Union, to keep records according to paragraph 8 on the recipient of the payment of the cross-border payment and on the cross-border payment in connection with the payment service provided, namely for the period of the calendar quarter during which he provided payment services corresponding to more than 25 cross-border payments to the same payee. The number of cross-border payments according to the first sentence is determined according to the payment services provided by the domestic payment service provider and according to the identifiers listed in paragraph 7. If the domestic payment service provider has information that the payee has several identifiers, the number of cross-border payments is determined according to the payee.
- (3) The obligation according to paragraph 2 applies to the domestic payment service provider
- a) payee,
- b) the payment provider, if none of the payee's payment service providers is located in the territory of the European Union.
- (4) In order to determine the number of cross-border payments according to paragraph 2, the domestic payment service provider of the payment provider according to paragraph 3 letter b) obliged to include all payment services provided to the payment provider that correspond to cross-border payments to the same payee.
- (5) The domestic provider of payment services according to paragraph 3 is obliged
- a) keep records according to paragraph 8 in electronic format for a period of three calendar years from the end of the calendar year in which the payment was made,
- b) to make available to the financial directorate by electronic means the records according to paragraph 8 through an electronic form no later than the end of the calendar month following the calendar quarter to which these records relate according to a special regulation. ^{28p)}
- (6) For the purposes of this provision, the location of the payment provider that makes the cross-border payment is considered to be the Member State identified under
- a) IBAN of the payment provider's payment account or any other identifier that determines the payment provider and its location, or
- b) BIC or any other business identification code that determines the payment service provider acting on behalf of the payment provider and its location, if identifiers according to letter a) are not available.
- (7) A member state or a third state identified by
- a) IBAN of the payee's payment account or any other identifier that determines the payee and his location, or
- b) BIC or any other business identification code that determines the payment service provider acting on behalf of the payee and its location, if identifiers according to letter a) are not available.
- (8) The records according to paragraph 2, which the domestic payment service provider is obliged to keep according to paragraph 3, must contain
- a) BIC or any other business identification code that identifies the payment service provider,
- b) name and surname of the payee or trade name or name of the payee, listed in the records of the payment service provider,
- c) tax identification number or national tax number of the payee, if available,
- d) IBAN or any other identifier that determines the payee and his location, if the IBAN is not available,
- e) BIC or any other business identification code that identifies the payment service provider acting on behalf of the payee and its location, if the payee receives funds and does not have a payment account,
- f) the address of the payee, if available, listed in the records of the payment service provider,
- g) data on all cross-border payments according to paragraph 2,
- h) data on returned payments related to cross-border payments according to letter g).
- (9) In the case of data according to paragraph 8 letter g) shall be stated
- a) date and time of payment,
- b) amount and currency of payment,
- c) the Member State of origin of the payment accepted by the payee or received on behalf of the payee, and the type of identifiers according to paragraph 6 used for the purpose of determining this Member State,

For non-fulfilment of tax obligations, the tax administrator imposes or collects a fine on the tax subject for an administrative offense if:

j) does not fulfill any of the obligations of a non-monetary nature according to this Act, while it is not an administrative offense according to letters a) to i), e.g. failure to submit a summary statement, report - fine from 60 euros to 3,000 euros.

For the commission of an administrative offense, the tax administrator imposes fines, while he does not impose a fine if it does not exceed 5 euros, and if the tax administrator is a municipality, if it does not exceed 3 euros.

With the amendment to the tax code effective from 1 January 2024, the tax administrator takes into account the severity, duration, and consequences of the illegal situation and the tax reliability index when determining the amount of the fine. The tax office or the customs office will not impose a fine, the amount of which can be determined within the established range, for the first violation of the obligation, the institute of the so-called "second chance". It will be used for the imposition of a fine if the fact decisive for the imposition of the fine occurred after 31.12.2023.

According to the national expert, Slovakia **has not adopted the MOSS Scheme**; and it is **not necessary to involve more PSPs on the fight against VAT fraud**.

Slovenia

Slovenia **is compliant with Directive 2020/284**. The implementation came into force on 1 January 2024. Regarding the Mini One-Stop Shop (MOSS) scheme, Slovenia has been **proactive in adopting electronic invoicing and reporting obligations**.

Spain

Spain **complies with Directive 2020/284**, which was transposed into national law through Law 11/2023, Section III. These provisions came into force on January 1, 2024. **Prior to this, Spanish legislation did not impose obligations on Payment Service Providers (PSPs)**. As a result of this implementation, PSP obligations are now outlined in Articles 166 ter to quinquies of the VAT Law (Law 37/1992 of December 28, 1992, as amended by Law 11/2023 of May 8) and are further detailed in Articles 62 ter and 81a of the VAT Regulation (Royal Decree 1624/1992 of December 29, 1992, approving the Value Added Tax Regulation, as amended by Royal Decree 1171/2023 of December 27).

Non-compliance with these obligations constitutes a tax infringement under Article 200.1(c) of the General Tax Law (Law 58/2003 of December 17, 2003), which addresses failures to maintain required accounting records and systems. Penalties for such infringements include:

-
- d) any information that identifies the payment,
 - e) information about the payment made on the premises of the supplier of goods or services, if the payment service provider is aware of it.
- (10) In the case of data according to paragraph 8 letter h) shall be stated
- a) date and time of payment refund,
 - b) the amount and currency of the returned payment,
 - c) the Member State of destination of the returned payment and the type of identifiers according to paragraph 6 used for the purpose of determining this Member State.

- **A fixed pecuniary fine** of €150.
- For **serious breaches, a proportional fine of 1%** of the offender's turnover for the relevant financial year, with a minimum of €600.

Additionally, manufacturing, producing, marketing, or possessing accounting software that allows for the manipulation of financial records is considered a serious tax infringement under Article 201 bis of the General Tax Law. Penalties for this include fines ranging from €50,000 to €150,000.

It's important to note that the possession of non-compliant accounting software by users is also subject to penalties, which can range from €1,000 to €50,000, depending on the severity of the non-compliance.

Spain has adopted the MOSS Scheme.

According to the national expert, financial service providers are in a privileged position to identify suspicious activities related to VAT fraud due to their access to detailed financial data and transactions. Therefore, financial service providers can be of great help in the fight against tax fraud if they cooperate with the authorities in this regard. However, encouraging such collaboration can be difficult. Some suggestions could include:

- **provide training to employees of financial service providers** so that they are alert to potential indicators of VAT fraud and know how to report them properly.

Consequently, **establish procedures for financial service providers to report any suspicious activity** to the competent authorities.

Sweden

Sweden is **compliant with Directive 2020/284**. Before this, Swedish legislation did not impose obligations on Payment Service Providers (PSPs).

In Sweden, **administrative sanctions are imposed on payment service providers (PSPs) that fail to meet record-keeping and reporting obligations**. Two distinct charges apply:

- **Documentation Charge (Record-Keeping Charge).**
 1. **Rate:** 0.3% of the PSP's turnover from the previous financial year.
 2. **Minimum:** SEK 3,000.
 3. **Maximum:** SEK 3 million.
 4. **Condition:** Applied when a PSP fails to maintain the required records.
- **Reporting Charge.**
 1. **Rate:** 0.1% of the PSP's turnover from the previous financial year.
 2. **Minimum:** SEK 1,000.
 3. **Maximum:** SEK 1 million.
 4. **Condition:** Applied when a PSP fails to submit the required reports within the specified timeframe.

Both charges are mutually exclusive within the same reporting period; only one can be levied, depending on the nature of the non-compliance.

Sweden has adopted the MOSS Scheme.

According to the national expert, it would be better to have this adoption mandatory and not optional. Additionally, when **new reporting requirements are introduced, they usually require significant initial adaptation of IT and reporting systems, which can be costly**. However, once the systems are in place, the ongoing burden is minimal.

It would be very important to improve **PSPs sharing information**, as it can be valuable in combating VAT fraud since PSPs already possess much of the necessary data.

In Sweden, **the decisions of the tax authorities are publicly available for all to see**, and therefore you can actually control them. Finally, another suggestion can be to **extend the OSS Scheme to all B2C transactions within the EU. Collaborate with more non-EU countries with the aim of enabling the application of OSS also with some non-EU countries**, for example with Norway, Island and Lichtenstein, and maybe Switzerland.

6.3 Anti-fraud cycle and the role of the private sector in combating and preventing cyber-VAT fraud VAT

The engagement of private sector **Payment Service Providers (PSPs)** in the prevention and detection of VAT fraud has garnered significant attention from national experts and stakeholders across the EU, revealing a spectrum of perspectives regarding their optimal involvement. Several Member States, including Malta, Lithuania, and Luxembourg, emphasize that PSPs already bear substantial reporting obligations. Consequently, the focus should prioritize the effective utilization of existing data rather than imposing additional burdens. This viewpoint is echoed by Hungary, which warns against exacerbating PSPs' reporting responsibilities, highlighting the sufficiency and efficiency of current frameworks. Conversely, countries such as Romania and Belgium identify the primary challenge as the tax authorities' limited capacity to process and interpret the extensive data currently provided, rather than a deficiency of information itself. Finland and Lithuania further advocate for a thorough evaluation of the existing legal and reporting mechanisms before introducing supplementary obligations.

The Netherlands draws attention to Directive 2020/284, which mandates PSPs to report transaction data to tax authorities, with reporting frequency determined by Member States. It was suggested that instituting a mandatory, real-time reporting system akin to e-invoicing could enable more immediate detection and response to fraudulent VAT activities. Similarly, Latvia posits that PSPs and related service entities could assume a more proactive role in early fraud detection and overall preventive efforts.

Other Member States emphasize complementary measures, such as Spain and France's calls for enhanced training of financial institution personnel to identify and report suspicious transactions. Sweden and the Czech Republic propose expanding the One Stop Shop (OSS) mechanism and designating platforms as deemed suppliers to simplify VAT collection processes and curtail fraud opportunities. Greece and Germany advocate for the adoption of risk-based approaches aligned with anti-money laundering frameworks, leveraging similar criteria to identify illicit conduct. Croatia specifically recommends real-time reporting for cross-border B2B transactions to improve transparency and oversight.

Underlying these suggestions is a widely shared recognition of the necessity for improved collaboration and communication between PSPs and tax authorities, with Spain and France among those advocating for structured channels and shared accountability.

Unanimity was achieved on the importance of a balanced approach that combines compliance, data accessibility, and clear liability frameworks to enhance the effectiveness of PSPs' contribution to VAT fraud mitigation. Given the recent introduction of new storage and reporting obligations for PSPs, ongoing dialogue and refinement of these strategies remain imperative to harmonize practices across Member States.

Ultimately, consensus emerged around the potential benefits of transitioning to a mandatory OSS system, which could streamline VAT collection, improve compliance, and foster greater uniformity within the EU. Continued engagement and feedback from stakeholders will be crucial to advancing this agenda and addressing the complexities inherent in integrating the private sector into VAT fraud prevention frameworks.

7. Recommendations and proposals to improve anti-fraud strategies against cyber-VAT fraud

7.1 Substantive criminal law

Harmonisation, legal convergence and integration in the EU

Both from the analysis of the literature on the subject (Foffani et al., 2019; Farkas et al., 2019; European Commission – OLAF Bernardi&Negri, 2015) and from what emerged from the first online focus group conducted together with the selected national experts reveal the cross-border nature of cyber VAT fraud and the need for stronger EU-level coordination.

The **PIF Directive** (Directive (EU) 2017/1371 on the fight against fraud to the Union's financial interests by means of criminal law) remains essential for defining and prosecuting offences that harm the EU budget. By setting a baseline for the criminalisation of fraudulent conduct and associated sanctions, it aims to foster coherence among national systems and enhance cross-border cooperation. Its importance is heightened by the growing complexity of fraud schemes and the scale of EU funding distributed through mechanisms such as the Recovery and Resilience Facility. Ensuring that the Directive is fully and effectively implemented is thus critical to upholding the rule of law, ensuring financial accountability, and reinforcing mutual trust among Member States.

The Directive already provides for, and indeed anticipates, a process of harmonisation among Member States' criminal law frameworks. However, as demonstrated in the preceding legal analysis, while there is a generally high level of formal compliance—particularly with key provisions such as **Article 3** (concerning VAT fraud committed by natural persons), **Article 7** (sanctions on natural persons), **Article 6** (liability of legal persons), and **Article 9** (sanctions on legal persons)—the harmonisation process remains incomplete.

In addition, the Directive establishes only **minimum standards**, leaving significant room for variation in implementation, interpretation, and enforcement at the national level. This divergence risks undermining the effectiveness of the EU's collective efforts to protect its financial interests and ensure the consistent application of criminal law across the Union.

There are also divergences concerning the subjective element of the offence: in some Member States, criminal liability is established for both intentional and negligent conduct. Several experts have highlighted the need for a **harmonised approach to criminal liability** that extends beyond intentional misconduct to include cases of negligence where appropriate. This would ensure a broader scope of accountability for actions that harm the financial interests of the European Union.

Moreover, **Member States should be strongly encouraged to explicitly incorporate aggravating circumstances** for VAT fraud committed by organised criminal groups, in full alignment with Article 8 of the PIF Directive, rather than relying solely on general aggravating provisions applicable to all offences. Indeed, **large-scale cross-border VAT fraud schemes are often orchestrated by organised**

criminal networks, which operate not only to generate illicit profits but also to launder the proceeds of other criminal activities.

In view of the above, the policy recommendations to strengthen harmonisation, legal convergence and integration in the EU are as follows:

1. Strengthen enforcement and monitoring of the PIF Directive

To promote uniform and effective implementation across the EU, the **European Commission** should strengthen its monitoring, evaluative, and support mechanisms—particularly in Member States where compliance is partial, ambiguous, or not fully aligned with the Directive’s intent. This may involve a multi-faceted approach that includes the provision of targeted **legal and technical assistance**, tailored to the specific legislative and institutional challenges faced by individual Member States.

2. Promote further harmonisation of the subjective element of the VAT-related offences

Entourage MSs to adopt a more harmonised approach to criminal liability, including **negligent conduct** where justified, in line with expert recommendations and the evolving complexity of fraud schemes.

3. Ensure pacific aggravating circumstances for organised VAT fraud

As foreseen in **Article 8 of the PIF Directive**, rather than relying solely on general provisions.

4. Institutionalise per-learning and knowledge-sharing platforms

The **European Commission** could expand and formalise **peer-learning platforms** more broadly as a strategic tool to support the implementation of EU legal instruments, particularly in areas requiring close coordination between national legal systems and EU law. Such platforms would enable national authorities to exchange best practices, clarify interpretative challenges, and work towards greater convergence in the practical application of EU legislation.

5. Broaden and systematise stakeholder engagement

Within the context of EU cyber VAT project, the exchange of knowledge and perspectives among national experts and stakeholders proved to be both **valuable and insightful**, contributing meaningfully to mutual understanding. However, these exchanges were **limited in scope and scale**, underscoring the need for more systematic, structured, and inclusive mechanisms of engagement. It is therefore essential that future initiatives ensure the **broad and sustained involvement of diverse stakeholders**. Bringing together these varied perspectives can foster a more comprehensive understanding of the challenges faced by Member States in implementing EU law and can help identify practical solutions grounded in real-world experience.

Institutionalising such dialogue beyond ad hoc consultations or project-based activities, the EU could enhance **mutual trust, legal coherence, and administrative capacity** across Member States. In doing so, peer-learning platforms would not only serve the transposition and enforcement of specific directives like the PIF Directive, but also contribute to the **overall strengthening of the EU’s legal and governance architecture**, particularly in areas involving complex cross-border cooperation and shared competences, as it is the protection of the European Union’s financial interests.

Regulatory reforms

A critical discussion on the need for regulatory reform emerged from both the analysis of relevant literature (Farkas et al., 2019; Lasagni, 2015; Llopis-Gilabert et al., 2022) and the insights gained during the first online focus group with selected national experts, particularly concerning the potential introduction of a new offence specifically addressing cyber VAT fraud.

The majority of Member States consider cyber VAT fraud to fall under the traditional category of VAT fraud, owing to the inherently adaptable and free-form nature of the offence. The prevailing consensus among national experts is that **introducing a distinct criminal offence specifically for cyber VAT fraud is unnecessary, highlighting the need for regulatory reform that extends beyond the mere creation of new criminal categories.** Cyber VAT fraud is largely regarded as a technological evolution of traditional VAT fraud, which can be effectively addressed within the existing legal frameworks. However, some experts suggest that it may be appropriate to introduce an **aggravating circumstance for VAT fraud cases involving the use of cyber elements**, in order to reflect the increased complexity and potential impact of such offences.

There is a shared understanding that the creation of new criminal offences or the classification of cyber elements as aggravating circumstances may, in any event, be less effective than investing in the strengthening of investigative and technical capacities. In particular, the development of **real-time monitoring tools, advanced data analytics (including those powered by artificial intelligence), and interoperable systems capable of supporting efficient cross-border enforcement is considered a more pragmatic and impactful approach.** These dimensions—specifically relating to cross-border cooperation and the use of technological tools in criminal investigations—will be examined in greater detail in the following sections, as they represent key recommendations that emerged throughout the course of this project.

From a structural legal perspective, it is also important to recognise that in many Member States, VAT fraud is not codified as a distinct criminal offence but is instead subsumed under broader categories such as general fraud or tax evasion. As a result, introducing a specific offence for cyber VAT fraud would not only be unnecessary but also incompatible with certain national legal systems. **Rather than creating a cyber-specific offence, the priority should be to establish a clear, harmonised definition of VAT fraud at the EU level.** Such harmonisation would enhance legal clarity, improve judicial cooperation, and support more consistent enforcement practices across Member States.

Discussions among national experts also revealed a strong consensus that **administrative liability for legal persons is often more effective than criminal liability in addressing VAT fraud.** Administrative frameworks are generally better equipped to promote corporate compliance, deliver proportional and timely sanctions, and mitigate the risks associated with over-criminalization. Consequently, to enhance the efficiency and proportionality of enforcement in VAT fraud cases, **Member States should be encouraged to strengthen their administrative liability regimes for legal persons, ensuring these are robust, dissuasive, and consistently enforced.** Such an approach can increase compliance levels while alleviating pressure on national criminal justice systems.

According to some stakeholders, a further regulatory reform in the area of fiscal policy could involve the implementation of a **generalized split payment regime, particularly targeted at sectors traditionally characterized by a higher incidence of VAT fraud.**

In light of the above, the policy recommendations aimed at regulatory reforms, are as follows:

1. Do not introduce a separate offence for cyber VAT fraud

Maintain cyber VAT fraud within the broader category of VAT fraud, recognising its nature as technological evolution of existing criminal behaviours. Avoid fragmentation and potential conflict with national legal systems where VAT fraud is not codified as separate offence

2. Harmonise the definition of VAT fraud at the EU level

Work toward establishing a **uniform, EU-level definition of VAT fraud to enhance legal clarity, judicial cooperation and consistent enforcement** across MSs

3. Consider cyber elements as aggravating circumstances

Encourage Ms to include **explicit aggravating circumstances for VAT fraud committed using cyber tools or digital platforms**, to reflect increased sophistication and impact

4. Prioritise investment in investigative and technological capacities

Promote the development and employment of **real-time monitoring tools, Ai powered data analytics, interoperable systems that facilitate cross-boarder cooperation** in criminal investigations

5. Strengthen administrative liability regimes for legal persons

Reinforce administrative liability frameworks that are robust, dissuasive and consistently applied; leverage administrative mechanisms to **increase corporate compliance** and reduce the burden on criminal justice systems

6. Explore fiscal policy measures such as sector-specific split payment regimes

Assess the potential of introducing **generalised or sectors-specific split payment regimes**, as part of a preventive regulatory strategy

7.2 Criminal procedure and investigations

Specialised and more efficient investigations

As previously noted, the introduction of a new category of criminal offence for cyber VAT fraud does not appear necessary. Rather, the primary challenge in this domain—consistent with broader trends in cybercrime—concerns the investigative phase. The detection and collection of evidence are significantly complicated by the inherently immaterial, digital, and often transnational nature of such offences. This complexity suggests that establishing new offences or classifying cyber elements as aggravating circumstances would be less effective than investing in the enhancement of investigative and technical capabilities.

A broad consensus among experts supports the view that the creation of specialised investigative units, the upgrading of technical resources, and the deployment of advanced digital tools represent more practical and impactful strategies for addressing cyber-enabled VAT fraud. Even in instances where digital components are integral to the commission of the offence, as is characteristic of cybercrime in its broader sense, priority should be given to improving the regulation of investigative procedures—particularly those related to the collection, processing, and analysis of electronic evidence. There is a clear and growing need for real-time monitoring tools, sophisticated data

analytics (including AI-driven technologies), and interoperable systems capable of supporting effective cross-border cooperation and enforcement.

According to stakeholders and the national experts, to enhance the effectiveness and coherence of VAT and cyber VAT fraud enforcement across the European Union, a set of institutional, legal, and procedural reforms should be prioritised. Two overarching areas emerged as particularly significant from the comparative analysis of Member States' responses and expert discussions, specialised training, institutional capacity building and legal harmonisation and procedural reform.

In order to assure specialised and ore efficient investigations:

1. Invest on specialised training and specialise investigative unit

Many Member States stressed the urgent need for **comprehensive training programmes** and structural reforms aimed at equipping investigators, prosecutors, and judges with specialised knowledge in economic crime and cyber fraud; develop **minimum standards for institutional capacity**, including trained personnel in cyber investigation, economic crime analysis, and digital evidence handling. Notably, not all Member States currently possess specialised law enforcement bodies dedicated to economic and fiscal crime, which in some cases creates significant obstacles to the effective investigation and prosecution of VAT fraud. Strengthening institutional capacity through dedicated units is therefore essential to ensure more consistent and efficient enforcement across the EU.

2. Promote EU-wide specialised training and curricula

Development of national and EU-wide curricula, support for cross-border secondments and exchanges, and the establishment of dedicated fiscal crime units with interdisciplinary expertise in law, finance, and digital technologies. Propose the creation of an EU Training Centre for Financial and Cyber Crime, possibly under the aegis of CEPOL or Eurojust, to coordinate **standardised curricula, cross-border secondments, and knowledge exchange**.

3. Enhance procedural harmonisation

Revise existing EU instruments (e.g., the European Investigation Order, the PIF Directive) to include **minimum procedural guarantees**, shared evidentiary thresholds, and access to digital investigative tools, particularly in terms of available tools, evidentiary standards, and investigative powers. Once more, the lack of coherence across Member States hampers the effectiveness of cross-border investigations and creates disparities in enforcement.

4. Encourage the establishment of specialised judicial tracks

Provide EU funding and best-practice guidelines for the establishment and operation of financial crime chambers within national judicial systems.

5. Align statutes of limitations with complexity of transnational crime

Implement minimum limitation periods consistent with Article 12 of the PIF Directive, ensuring sufficient timeframes for investigations to unfold.

6. Align statutes of limitations with complexity of transnational crime

Implement minimum limitation periods consistent with Article 12 of the PIF Directive, ensuring sufficient timeframes for investigations to unfold.

Use of technology in prevention and investigations

Law enforcement authorities across the European Union employ a diverse array of investigative tools to combat VAT fraud, adapting these instruments to national legal frameworks while converging around common European standards. National experts consistently report that investigative practices—such as data analytics, risk-based audits, search and seizure operations, and inter-agency cooperation—remain foundational in addressing both traditional and cyber-enabled forms of VAT fraud. Though not originally designed for cybercrime, these tools are increasingly adapted to address the evolving digital nature of VAT fraud.

A broad consensus among Member States and experts suggests that the emergence of cyber VAT fraud does not necessitate entirely new investigative categories. Rather, the primary challenge lies in modernising and strengthening existing mechanisms to make them fit for purpose in the digital age. This includes enhanced forensic capacities to gather and process digital evidence, expanded use of automated screening tools such as VIES, and the application of advanced surveillance techniques and witness interviews in technologically complex cases.

Cross-border cooperation remains a cornerstone of effective investigation due to the transnational character of VAT fraud schemes. Joint task forces, intelligence-sharing platforms, and harmonised procedures play a key role in overcoming jurisdictional and legal obstacles. However, various national experts and stakeholders, and the academic literature (Merkx & Verbaan, 2019; OECD, 2017;) underscore the need for deeper technological integration, improved investigative coordination, and legal innovation.

Furthermore, ICT policies across the EU remain fragmented. While all Member States maintain ICT crime strategies, relatively few explicitly address VAT fraud—and fewer still focus on cyber VAT fraud. There is widespread recognition of the need to better harness technological infrastructure and to develop cohesive policy frameworks that respond to the specificities of cyber-enabled tax offences.

Among the key recommendations are:

1. Technological modernisation of investigative tools

- Invest in AI-based anomaly detection, real-time transaction monitoring, and digital forensics tools—including lawful hacking—for complex VAT fraud investigations.
- Facilitate the integration of **risk-based and automated audit systems to proactively detect suspicious behaviour.**

2. Interconnection of National data systems

- Promote the development of **interoperable databases across Member States** to enable seamless data cross-checks.
- Establish secure channels for real-time data exchange between tax administrations and law enforcement bodies.

3. Harmonisation of digital infrastructures

- Create **EU-wide digital platforms for investigative coordination**, reducing inefficiencies caused by nationally fragmented ICT systems. Develop common technical standards and legal protocols for digital evidence handling and cyber-enabled investigations.

4. Specialised Training and Dedicated Units

- Encourage Member States to establish fiscal crime units with cross-disciplinary expertise in law, finance, and digital technology.
- Support the development of **EU-level training curricula** focused on cyber VAT fraud investigation and digital evidence management.

5. Digital Standardisation for E-Reporting and E-Invoicing (see below)

- Prioritise the **standardisation of digital reporting systems at the EU level**, ensuring coherence, efficiency, and low implementation burdens for businesses.
- Ensure that implementation is proportionate, particularly for SMEs, and supported by EU-level guidance and funding mechanisms.

6. Ethical and Legal Governance of Technological Tools

- Establish regulatory frameworks to oversee the deployment of AI and surveillance tools, **ensuring compliance with EU data protection law and maintaining public trust, in full respect of the balance of fundamental rights and in alignment with the evolving European regulatory framework on artificial intelligence.**

AI technologies should be regulated within this normative context, not only to ensure legal and ethical oversight, but also to clarify their appropriate use in VAT fraud investigations. AI can serve as a valuable tool for anomaly detection and early-stage risk assessment; however, it must be complemented by human validation and oversight to avoid automated bias or false positives.

The use of AI in this domain should be understood as instrumental to strengthening the guarantees of the investigative process—not replacing it—and as a means to support, rather than substitute, traditional forensic and judicial procedures.

A key structural challenge is the absence of common datasets suitable for training and calibrating AI systems. Not only is there no EU-wide database for VAT-related investigations, but significant fragmentation also persists within individual Member States. It is therefore necessary to identify or construct interoperable baseline datasets that can support effective, accountable, and harmonised AI deployment across jurisdictions.

Effective use of reporting systems

Building on insights from both the literature and expert consultations, it is increasingly recognised that real-time reporting mechanisms—such as the Transaction Network Analysis (TNA), the VAT Information Exchange System (VIES), and the One-Stop Shop (OSS)—alongside comprehensive e-invoicing systems, constitute critical components in the prevention and early detection of cyber VAT fraud, particularly in the context of cross-border digital commerce. As highlighted by Llopis-Gilabert et al. (2022), these tools enhance fiscal transparency and reduce the latency between taxable transactions and enforcement actions, thereby limiting the window of opportunity for fraudulent conduct. Focus group discussions within this project echoed similar conclusions, stressing that the successful implementation of real-time data exchange mechanisms at the EU level would significantly strengthen the Union’s ability to monitor intra-community transactions and uncover fraudulent patterns.

Additional research supports this view. Merkkx and Verbaan (2019) argue that real-time access to transaction-level data allows tax authorities to move from reactive to proactive fraud detection models. Similarly, the OECD (2017) has emphasised the benefits of e-invoicing and digital reporting systems in reducing VAT compliance gaps and increasing traceability. Experts consulted during this study also highlighted the necessity of harmonising these digital infrastructures across Member States to avoid fragmentation and jurisdictional loopholes. Crucially, the burden of compliance—particularly for small and medium-sized enterprises (SMEs)—must be managed carefully to prevent unintended economic disadvantages. In this respect, simplified reporting regimes and technical support structures for SMEs are recommended.

Finally, the deterrent effect of fast and visible monitoring systems was a recurring theme in the discussions. Visible enforcement backed by technological sophistication not only improves the likelihood of detection but also reinforces taxpayer trust and voluntary compliance. These findings support the policy recommendation to accelerate the development and implementation of interoperable, real-time VAT monitoring tools at the EU level, accompanied by adequate safeguards for data protection and administrative feasibility.

In light of the above, the policy recommendations aimed at effecting using exporting systems, are as follows:

1. Accelerate the EU-Wide Implementation of Real-Time VAT Reporting Mechanisms

The European Commission should propose a **legislative roadmap mandating minimum real-time reporting capabilities**, supported by dedicated funding for Member States' digital infrastructure upgrades.

2. Promote Harmonisation of E-Invoicing and Digital Reporting Infrastructures

Develop a **common EU e-invoicing standard** (possibly through an update of the VAT Directive), ensuring technical compatibility and alignment with existing initiatives like PEPPOL and the ViDA (VAT in the Digital Age) proposals.

3. Transition Tax Authorities from Reactive to Proactive Fraud Detection Models

Provide EU-wide **technical guidance and shared services** (e.g., via Eurofisc or a centralised EU platform) to lower the entry barrier for less digitally advanced tax authorities.

Judicial cooperation

A recurring theme emerging from both the expert consultations and literature review is the critical importance of harmonisation and mutual recognition mechanisms across Member States to address cyber-enabled VAT fraud effectively. While full legislative harmonisation remains complex due to the diversity of national legal systems and sovereignty concerns, national experts and researchers consistently stressed the necessity of establishing common operational standards and fostering mutual trust. This form of **horizontal cooperation**—grounded in shared principles, interoperable procedures, and cross-border recognition of investigative actions—is essential to mitigate fragmented enforcement and enhance the effectiveness of the EU's overall fraud response.

In this context, the **pivotal role of the European Anti-Fraud Office (OLAF)** was strongly emphasised. Experts agreed that OLAF is uniquely positioned to act as a central hub for the coordination of cross-border investigative efforts and the circulation of evidence among Member States. However, to fulfil this role more effectively—especially in cases involving digital and transnational

dimensions—there is a clear need to strengthen OLAF’s investigative mandate, while simultaneously ensuring that such expansion respects the principles of subsidiarity and national sovereignty.

From a policy perspective, the European Commission should consider adopting a dual-track strategy. This would involve:

- a) **Enhancing administrative and technical enforcement capacities at the national level**, especially in terms of technological infrastructure and data integration; and
- b) **Reinforcing OLAF’s operational and investigative powers**, particularly for coordinating and supporting multi-jurisdictional investigations into VAT fraud and cyber-related offences.

To achieve this, the following policy recommendations are proposed:

1. Strengthen Cross-Border Investigative Cooperation

- Promote the broader and more systematic use of the **European Investigation Order (EIO)** to streamline the exchange of digital evidence and facilitate timely investigative actions across jurisdictions.
- Encourage the development of **harmonised reporting and audit systems**, supported by unified data-sharing protocols that ensure compatibility and legal reliability across Member States.
- Consider establishing **mutual recognition mechanisms for administrative and evidentiary procedures**, to avoid duplication and conflicting outcomes.

2. Expand OLAF’s Investigative Capacity

- Broaden OLAF’s mandate to include **more proactive investigative powers**, especially in areas involving cyber-enabled fraud, while maintaining appropriate checks to safeguard national competencies.
- Allocate targeted resources to OLAF for investment in **digital forensics, AI-driven data analytics, and secure cross-border communication tools** to support complex investigations.
- **Facilitate joint investigation teams (JITs)** where appropriate, coordinated by OLAF and involving relevant national agencies, to improve the handling of high-risk, high-value fraud cases.

3. Promote Data Integration and Interoperability

Some countries highlighted the strategic need for better integration of national data systems, such as:

- Develop **centralised databases** accessible to authorised tax authorities, financial intelligence units, and law enforcement agencies, ensuring real-time information exchange. It would be very important also to enhance the exchange of tax information between revenue authorities. While these bodies are not investigative per se, they often play a key role in identifying tax fraud, and faster information exchange could significantly improve detection efforts.
- Ensure these systems are **interoperable and secure**, incorporating functionalities for automated anomaly detection and **risk assessment tools** powered by machine learning.

- Integrate multiple data sources, including **e-invoicing platforms, digital payment systems, and customs databases**, to create a comprehensive overview of transactional behaviour and detect patterns indicative of VAT fraud.
4. Balance Efficiency with Safeguards
- Introduce **standardised audit and accountability frameworks** to govern data access and use, ensuring proportionality and protecting individual and corporate rights.
 - Offer **guidance and training** for national agencies and OLAF personnel on the ethical and legal dimensions of cross-border digital investigations.

7.3 Payment service providers and platform obligations

The introduction of **Directive (EU) 2020/284** represents a major development in the European Union's strategy to address VAT fraud in the rapidly evolving digital economy. The Directive requires **payment service providers (PSPs)** to collect and report detailed data on cross-border payments, including information on payers, payees, and transactions. This data is intended to be shared with national tax authorities, enabling them to better detect, monitor, and prevent VAT fraud, particularly in the context of e-commerce. Despite a general alignment, implementation has revealed **divergent approaches** to enforcement. Sanctions for non-compliance vary significantly across MSs, ranging from **administrative fines** to **criminal penalties**, including **non-monetary measures** such as public disclosure or imprisonment in severe cases. However, across the board, administrative sanctions are increasingly recognised as more **effective, proportionate, and enforceable**, especially in the context of financial transactions.

A number of critical insights emerged from the focus groups, national responses, and the literature (Merkx & Verbaan, 2019; OECD, 2017; Künnapas et al., 2025):

- **Data availability vs. processing capacity:** Many experts agreed that the key issue is not a lack of transaction data, but the limited ability of tax authorities to process, cross-reference, and extract actionable intelligence from this information. This fragmentation is evident not only across different countries but also within individual Member States, where coordination challenges often arise between domestic authorities—for instance, between the *Guardia di Finanza* and the *Agenzia delle Dogane e dei Monopoli* in Italy.
- **Proportionality of obligations:** Some MSs cautioned against over-regulating PSPs. They advocated for a balanced approach that considers the administrative burdens already borne by service providers.
- **Real-time and harmonised reporting systems:** This consideration extends to PSPs as well, in light of the demonstrated effectiveness of such instruments, as outlined above.
- **Collaboration and communication:** There was broad consensus on the necessity of fostering structured cooperation channels between PSPs and tax administrations across MSs to promote mutual trust, reduce duplication, and enhance responsiveness. For this reasons, it would be important to develop **EU-wide protocols for data sharing**, cooperation agreements, and feedback mechanisms between PSPs and national authorities, ensuring consistent standards and secure data flows.

In light of the above, the policy recommendations aimed at giving a more important role of the PSPs, are as follows:

1. Strengthen the Data Processing Capacities of Tax Authorities

The European Commission should establish a **Digital VAT Intelligence Support Facility**, offering technical tools, shared algorithms, and analytics expertise to help Member States extract actionable insights from PSP data.

2. Promote Harmonised and Proportionate Sanctions Across Member States

The Commission should publish **non-binding guidelines** or a Commission Recommendation outlining best practices for **proportional sanctioning and discouraging criminal penalties unless clearly justified**.

Introduce **reporting thresholds**, simplified regimes, or phased obligations for PSPs based on size, transaction volume, or risk classification.

3. Improve Domestic Inter-Agency Coordination in VAT Fraud Enforcement

Encourage Member States to **designate a single point of contact or national coordination unit** for VAT fraud data processing and enforcement.

7.4 Concluding remarks

The fight against cyber VAT fraud, but also VAT fraud in general, requires a strategic shift from fragmented national responses to a more harmonised, intelligence-led, and technology-driven enforcement model at the EU level. While full legislative harmonisation remains complex due to divergent national legal systems, this study confirms that operational convergence, based on mutual trust and standardised practices, can significantly improve the effectiveness of cross-border investigations.

The central role of OLAF in coordinating investigations and facilitating the circulation of evidence has been widely acknowledged. However, there is a growing consensus among experts and national authorities on the need to enhance OLAF's investigative powers—especially in the digital realm—while fully respecting Member State sovereignty and the principle of subsidiarity. Strengthening OLAF's capacity must be paralleled by improved interoperability of national systems, broader use of existing tools like the European Investigation Order, and better coordination between administrative and judicial authorities.

Moreover, the obligations introduced under Directive (EU) 2020/284 for Payment Service Providers (PSPs) represent a pivotal step forward. Yet, their full potential can only be realised if these obligations are supported by harmonised administrative liability frameworks, real-time data access for authorities, and coordinated audit mechanisms across Member States. Emphasis should also be placed on proportionality: strengthening compliance and reporting without overburdening service providers or small businesses.




Finally, the conclusions of this analysis highlight three interrelated pillars for future policy development:





1. **Enhanced Horizontal Cooperation** – Through common standards, shared investigative practices, and mutual recognition of evidence, Member States can move toward operational harmonisation without requiring deep legislative change.

2. **Technological and Institutional Integration** – From centralised databases to AI-driven risk analysis tools, the integration of digital infrastructure must underpin VAT fraud prevention and enforcement across the EU.
3. **Balanced and Coordinated Enforcement** – A dual-track approach that reinforces both national administrative enforcement and EU-level investigative coordination will strengthen the overall integrity of the Union's financial interests.

In conclusion, effective prevention and repression of cyber VAT fraud will depend not on the proliferation of new offences, but on the smarter, more collaborative use of existing tools and competencies. Policymakers are therefore encouraged to invest in coordination, data-driven enforcement, and capacity building at both national and European levels.

7.5 Recommendations | Summary

Three Interrelated Pillars for Future Policy Development		
 Enhanced Horizontal Cooperation	 Technological and Institutional Integration	 Balanced and Coordinated Enforcement
Through common standards, shared investigative practices, and mutual recognition of evidence, EU Member States can move toward operational harmonisation without requiring deep legislative change.	From centralised databases to AI-driven risk analysis tools, the integration of digital infrastructure must underpin VAT fraud prevention and enforcement across the EU.	A dual-track approach that reinforces both national administrative enforcement and EU-level investigative coordination will strengthen the overall integrity of the Union's financial interests.

	Harmonisation, Legal Convergence and Integration in the EU <ul style="list-style-type: none"> Strengthen enforcement and monitoring of the PIF Directive Promote further harmonisation of the subjective element of the VAT-related offences Ensure pacific aggravating circumstances for organised VAT fraud Institutionalise peer-learning and knowledge-sharing platforms Broaden and systematise stakeholder engagement
	Regulatory Reforms <ul style="list-style-type: none"> Do not introduce a separate offence for cyber VAT fraud Harmonise the definition of VAT fraud at the EU level Consider cyber elements as aggravating circumstances Prioritise investment in investigative and technological capacities Strengthen administrative liability regimes for legal persons Explore fiscal policy measures such as sector-specific split payment regimes
	Investigations <ul style="list-style-type: none"> Develop minimum standards for institutional capacity Promote EU-wide specialised training and curricula Enhance procedural harmonisation Encourage the establishment of specialised judicial tracks Align statutes of limitations with complexity of transnational crime
	Use of Technology in Prevention and Investigations <ul style="list-style-type: none"> Technological modernisation of investigative tools Interconnection of National data systems Harmonisation of digital infrastructures Specialised Training and dedicated Units Digital standardisation for E-Reporting and E-Invoicing Ethical and Legal Governance of technological tools



Use of Reporting Systems

- Accelerate the EU-Wide implementation of Real-Time VAT Reporting Mechanisms
- Promote Harmonisation of E-Invoicing and Digital Reporting Infrastructures
- Transition Tax Authorities from reactive to proactive fraud detection models



Judicial Cooperation

- Strengthen Cross-Border investigative cooperation
- Expand OLAF's investigative capacity
- Promote Data integration and interoperability
- Balance efficiency with safeguards



Payment Service Providers and Platform Obligations

- Strengthen the data processing capacities of Tax Authorities
- Promote harmonised and proportionate sanctions across Member States
- Improve domestic Inter-Agency coordination in VAT Fraud Enforcement

Bibliography

- Ainsworth, R. T. (2006). Carousel Fraud in the EU: A Digital Vat Solution. *Tax Notes International*, May 1, 2006, 443. Boston Univ. School of Law Working Paper No. 06-23. Retrieved from <https://ssrn.com/abstract=924189>
- Albrecht, H. J. (2008). *Postmodern Criminology and the Penal State*. In M. Dellwing & T. Schiller (Eds.), *Kriminologie im Umbruch. Verhandlungen der 31. Tagung der Kriminologischen Gesellschaft* (pp. 131–148). Forum Verlag Godesberg.
- Athanasiadou, N. (2021). VAT fraud and the involvement of organised crime groups: Typologies and investigation techniques. *ERA Forum*, 22(3), 447–460. <https://doi.org/10.1007/s12027-021-00666-0>
- Barker, J. C., & Stewart, A. (2021). Evasion or Avoidance? VAT and the Criminal Law. *Criminal Law Review*, (5), 399–412.
- Bernardi, A., & Negri, D. (Eds.). (2015). *Relationships between the national judicial authorities and the investigative agencies in the view of the EPPO: Operational models and best practices in fight against EU frauds (Booklet of the research, February – June 2015)*. University of Ferrara. Project financed by the European Commission – OLAF, Hercule III Programme (OLAF/2015/D1/006). Accessible at: <http://www.unife.it/progetto/olaf>
- Borselli, F. (2008). Pragmatic Policies to Tackle VAT Fraud in the European Union. *International VAT Monitor*, 5, 332–343.
- Borselli, F. (2011). Organised Vat Fraud: Features, Magnitude, Policy Perspectives. *Bank of Italy Occasional Paper No. 106*. Retrieved from <https://ssrn.com/abstract=1966015>
- Borselli, F., Di Nicola, A., & Vettori, B. (2015). Crypto-markets and illegal online trafficking of counterfeit medicines: A criminological analysis. *European Journal on Criminal Policy and Research*, 21, 389–408.
- Borselli, F., Fedeli, S., & Giuriato, L. (2015). Digital VAT carousel frauds: a new boundary for criminality? *Tax Notes International*, 707–724.
- Brunet, E. (2023). Crypto-assets and VAT: A European Analysis. *EC Tax Review*, 32(1), 5–11.
- CEPOL. (2022). *Carousel Fraud: Training Module*. European Union Agency for Law Enforcement Training.
- CESOP (2023). *Guidelines for the reporting of payment data*. Retrieved from https://taxation-customs.ec.europa.eu/taxation/vat/fight-against-vat-fraud/tackling-vat-fraud-e-commerce-cesop_en
- Chainey, S., & Berbotto, F. (2022). Crime scripting: Analysing organised crime in Italy. *Crime Science*, 11(1), 1–16.
- Chopin, J., & Beauregard, E. (2020). Script Analysis of Serial Sexual Offenders. *Journal of Criminal Justice*, 66, 101693.

- Clarke, R. V., & Newman, G. R. (2006). *Outsmarting the terrorists*. Greenwood Publishing Group.
- Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime Prevention Studies* (Vol. 3, pp. 151–196). Criminal Justice Press.
- Cornish, D. B., & Clarke, R. V. (2002). Analyzing Organized Crimes: A Crime Script Approach. In V. G. Smith & D. Cornish (Eds.), *Crime Prevention Studies* (Vol. 16, pp. 157–174). Criminal Justice Press.
- Di Nicola, A. (2022). Cyber-Organized Crime and Illicit Markets. In *Organized Crime in the 21st Century* (pp. 231–248). Springer.
- Economisti Associati, Oxford Research, CASE, Wavestone, Hedeos, Mazars, Desmeytere Services, & Università di Urbino. (2022). *VAT in the Digital Age - Volume 1 - Digital Reporting Requirements*. Retrieved from https://taxation-customs.ec.europa.eu/document/download/b09cd7eb-87ae-4317-beb8-4c0921d31353_en
- EPPO. (2024). *Annual Report 2023*. Retrieved from https://www.eppo.europa.eu/sites/default/files/2024-03/EPPO_Annual_Report_2023.pdf
- European Court of Auditors. (2019). *Special Report No. 12/2019: E-commerce – many of the challenges of collecting VAT and customs duties remain to be resolved*. Retrieved from <https://op.europa.eu/webpub/eca/special-reports/e-commerce-12-2019/en/>
- European Parliament. (2021). *Tackling VAT fraud in the EU*. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)698834](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698834)
- European Union. (2016). *Tackling intra-Community VAT fraud: More action needed*. Luxembourg: Publications Office of the European Union.
- European Union. (2024). *35th Annual Report on the Protection of the European Union's financial interests and the Fight against fraud 2023*. Report from the Commission to the Council and the European Parliament.
- European Union. (2024). *OLAF Report 2023*. Luxembourg: Publications Office of the European Union.
- Farkas, Á., Dannecker, G., & Jacsó, J. (Eds.). (2019). *Criminal law aspects of the protection of the financial interests of the European Union: With particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*. Wolters Kluwer Hungary Kft.
- Fedeli, S., Forte, F., & Reitano, A. (2011). EU VAT frauds: Economic and political issues. *European Journal of Law and Economics*, 32(2), 193–219.
- Foffani, L., Bin, L., Carriero, M.F. (2019). Cyber VAT frauds, ne bis in idem and judicial cooperation, A comparative study between Italy, Belgium, Spain and Germany. Research project, Giappichelli.
- Frunza, M. C. (2016). *Cost of the MTIC VAT Fraud for European Union Members*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2758566

- Frunza, M. C. (2018). *Value Added Tax Fraud*. Routledge.
- Gilmour, S. (2014). The role of financial crime scripting in preventing terrorist financing. *Journal of Money Laundering Control*, 17(3), 266–278.
- Griffioen M., van der Hel-van Dijk, E.C.J.M. (2016). Tackling VAT-Fraud in Europe: A Complicated International Puzzle. *Intertax*, Volume 44, Issue 4, 290 – 297.
- Hagan, F. E. (2011). *Research methods in criminal justice and criminology* (9th ed.). Pearson Education.
- Hancock, B., & Laycock, G. (2010). Organised crime and crime scripts: prospects for disruption. *International Journal of Police Science & Management*, 12(4), 345–355.
- Keen, M., Smith, S. (2006). VAT Fraud and Evasion: What Do We Know and What Can Be Done? (2006) in *National Tax Journal*, Vol. 59 (4), 861-887.
- KPMG (2000). E-Commerce and Cyber Crime: New Strategies for Managing the Risks of Exploitation. retrieved from: <https://www.uazuay.edu.ec/sites/default/files/public/E-Commerce%20and%20Cyber%20Crime.pdf>
- Künnapas, K., Maslionkina, P., Hinno, R., & Liberts, R. (2025). Current AI applications by Estonian tax authorities and use case scenarios. *TalTech Journal of European Studies*, 15(1[41]). <https://doi.org/10.2478/bjes-2025-0010>
- Lacoste, J., & Tremblay, P. (2003). Crime scripts: The case of cheque fraud. In M. J. Smith & D. B. Cornish (Eds.), *Crime Prevention Studies* (Vol. 16, pp. 169–192). Criminal Justice Press.
- Lagazio, M., Sherif, N., & Cushman, N. (2014). A multilevel approach to understanding the impact of cyber crime in the financial sector. *Computers & Security*, 45, 1–32. <https://doi.org/10.1016/j.cose.2014.04.006>
- Lamench, T. (2018). VAT and Missing Trader Fraud: EU Measures and National Responses. *World Journal of VAT/GST Law*, 7(2), 85–106.
- Lamensch, M., & Ceci, E. (2018). *VAT fraud – Economic impact, challenges and policy issues*. Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies. Retrieved from <https://www.europarl.europa.eu/cmsdata/156408/VAT%20Fraud%20Study%20publication.pdf>
- Lasagni, G. (2015). Cooperazione amministrativa e circolazione probatoria nelle frodi doganali e fiscali: Il ruolo dell'Ufficio europeo per la lotta antifrode (OLAF) alla luce della direttiva OEI e del progetto EPPO. *Diritto Penale Contemporaneo*.
- Lavorgna, A. (2013). The online trade of endangered species in Italy. *Crime Science*, 2(1), 1–12.
- Lavorgna, A. (2014). Wildlife trafficking in the Internet age. *Crime Science*, 3(1), 1–12.
- Leclerc, B., & Morgenthaler, S. (2023). Applying Crime Script Analysis to Cybercrime: A Systematic Review. *Aggression and Violent Behavior*, 65, 101805.

- Lee, J., & Holt, T. J. (2020). Cybercrime and Cryptocurrency: The role of technology in crime. *Deviant Behavior*, 41(4), 471–484.
- Llopis-Gilabert, B., Leal-Buenfil, R., & Pla-Julián, I. (2022). Fiscal and economic competition implications of carousel fraud in the European Union. *International Journal of Business & Management Studies*, 3(5).
- Mativat, S., & Tremblay, P. (1997). Electronic money and fraud: Lessons from the smart card industry. *Crime Prevention Studies*, 8, 173–197.
- Merkx, M., & Verbaan, N. (2019). Technology: A key to solve VAT fraud? *EC Tax Review*, 28(6), Kluwer Law International BV, 326-332.
- Michalik, T. (2017). *How the European Commission and European Countries Fight VAT Fraud* (Bank - CASE Seminar Proceedings 0147). CASE - Center for Social and Economic Research.
- Moiseienko, A. (2020). Cross-border VAT fraud and the misuse of online platforms. *RUSI Occasional Papers*.
- Morgenthaler, S., & Leclerc, B. (2023). Cybercrime and Crime Scripts: Typology and Theoretical Implications. *International Journal of Cyber Criminology*, 17(1), 1–24.
- Morselli, C., & Roy, J. (2008). Brokerage qualifications in ringing operations. *Criminology*, 46(1), 71–98.
- Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access*, 9, 163965–163986.
- OECD. (2017). *Technology Tools to Tackle Tax Evasion and Tax Fraud*. OECD Publishing.
- Papis-Almansa, M. (2019). VAT and electronic commerce: The new rules as a means for simplification, combatting fraud and creating a more level playing field? *ERA Forum*, 20, 201–223. <https://doi.org/10.1007/s12027-019-00575-9>
- Petrosino, A., & Brensilber, D. (2003). The role of crime scripts in understanding crime. *Journal of Community Psychology*, 31(5), 549–556.
- Sarnowski, J., & Selera, P. (2020). European compact against tax fraud—VAT solidarity and new dimension of effective and coherent tax data transfer. *ERA Forum*, 21, 81–93. <https://doi.org/10.1007/s12027-020-00603-z>
- Sarrica, F. (2005). Criminal networks and illegal immigration: The case of Italy. *Crime, Law and Social Change*, 43, 93–120.
- Savona, E. U. (2010). Organized criminal networks and their use of modern technology. *European Journal on Criminal Policy and Research*, 16(1), 89–105.
- Scarcella, L. (2020). E-commerce and effective VAT/GST enforcement: Can online platforms play a valuable role? *Computer Law & Security Review*, 36, 105371. <https://doi.org/10.1016/j.clsr.2019.105371>

- Sergiou, L. (2012). Value Added Tax (VAT) Carousel Fraud in the European Union. *Journal of Accounting and Management*, 2(2), 9–21.
- Signifyd. (2024). *The State of Fraud and Abuse 2024: The industrialization of online fraud has changed the rules — and the stakes — of the game*. Retrieved from https://resources.signifyd.com/first-party?utm_medium=press-release&utm_source=businesswire&utm_campaign=24Q3_NA_First-party-fraud
- Smith, R. G. (2005). Crime scripts and money laundering. *Journal of Money Laundering Control*, 8(4), 329–340.
- Smith, R. G. (2007). Missing Trader Intra-Community Fraud: A European Perspective. *Journal of Financial Crime*, 14(1), 40–47.
- Snaphaan, T., & van Ruitenburg, T. (2024). Script analysis in financial crime: A new approach to understanding money laundering. *Journal of Financial Crime*, 31(1), 1–18.
- SOCTA. (2013). *Serious and Organised Crime Threat Assessment*. Europol.
- Sokolovska, O. (2016). Cross-border VAT frauds and measures to tackle them. *Munich Personal RePEc Archive*. Retrieved from <https://mpra.ub.uni-muenchen.de/70504/>
- Tompson, L., & Chainey, S. (2011). Profiling illegal waste activity: using crime scripts to inform enforcement strategies. *European Journal on Criminal Policy and Research*, 17(3), 179–201.
- Tremblay, P., Talon, B., & Hurley, D. (2001). Body switching and related adaptations in the resale of stolen vehicles: Script elaboration and group decision making. *British Journal of Criminology*, 41(4), 561–579.
- Tundo, M. (2010). VAT fraud and the EU's response: A critical analysis. *Intertax*, 38(4), 206–218.
- Van Brederode, R. F. (2008). Third-Party Risks and Liabilities in Case of VAT Fraud in the EU. *International Tax Journal*, Jan–Feb, 31–42.
- Van der Bruggen, K., Roks, R., & Van Wijk, A. (2021). Organized crime and the use of violence: Script analysis of violent incidents in the Netherlands. *Crime, Law and Social Change*, 75(1), 83–105.
- Van Nguyen, D. (2022). Digital payment systems and fraud: Using crime scripts to analyse modus operandi. *Journal of Financial Crime*, 29(4), 1225–1239.
- Vanhoeyveld, J., Martens, D., & Peeters, B. (2020). Value-Added Tax fraud detection with scalable anomaly detection techniques. *Applied Soft Computing*, 86, 105904.
- von der Leyen, U. (2024). *Europe's Choice – Political Guidelines for the Next European Commission 2024–2029*. Retrieved from https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf
- Weirich, S. (2019). Script Analysis of Illicit Antiquities Trafficking. *Journal of Crime and Justice*, 42(1), 30–48.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organizational context. *Information and Organization*, 16(4), 304–324.

Annex I – Questionnaire for national experts

EU CYBER VAT

Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study

Union Anti-Fraud Programme (EUAF) - EUAF-2022-TRAI - 101101811

Questionnaire for National Experts | March 2024



With the financial support of the Directorate-General for European Anti-Fraud
Office – OLAF Union Anti-Fraud Programme – EUAF

Dear national expert,

first of all, thank you for taking on this task. This is the questionnaire you have been asked to complete as part of the project "EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study", which is co-funded by the EU Anti-Fraud Programme (EUFAP).

In the box below you will find an overview of the project.

1. Questionnaire's purpose

The purposes of EU CYBER VAT Questionnaire are the following:

- to present the state of play of the transposition of **Directive (EU) 2017/1371** of the European Parliament and of the Council of July 5, 2017 on the fight against fraud to the Union's financial interests by means of criminal law (hereinafter "**PIF Directive**") into the national law of the Member States and the mapping of the national legislation of the Member States in relation to the criminal offences of VAT fraud and cyber VAT fraud;
- to identify which **investigative tools/measures** are used in the EU Member States to investigate and prosecute VAT fraud and cyber VAT fraud;
- to examine the **role of ICT in the strategy / policy to combat cyber VAT fraud**;
- to assess the legal framework for **cyber-VAT Fraud** (e.g. MTIC) affecting the EU's financial interests in the context of **e-commerce**;
- to identify trends in (new) cybercriminal activities against the EU's financial interests by describing clusters of the modus operandi and of cyber VAT fraudsters in the EU based on **case studies**.

2. Instructions for completing the questionnaire

This survey contains two types of questions: closed and open.

You can select your answer by double-clicking on the appropriate box and then clicking on the "ticked" option. You can also simply write an "X" next to the box you want to check. If your answer is not listed in the options, please use the space in the table to write your answer.

For open questions, you can write your answer in the space next to the question. Please use as much space as necessary - the field will automatically expand to fit your answer.

Please answer **questions 1, 2 and 4** using the **Annexes**. We have carried out a preliminary analysis of EU Member States' national legislation based on desk research and ask you to confirm the results set out in the Annexes. Please use the Annexes to: a) confirm or deny the reported information; b) provide clarifications in case of non-confirmation through comments; c) provide us with an English version of the text of the relevant legislation.

Deadline: we kindly ask you to return the questionnaire to us by April, 30 2024 by sending it at: cssc@unitn.it

PROJECT OVERVIEW

1. Background

EU cyber-VAT fraud poses an increasing threat to the protection of the European Union's financial interests. Given the growth of the digital market and the **digitization of VAT-related operations**, the legal framework for VAT fraud at EU and Member State level must be adequate to also effectively prevent and combat criminal conduct in cyberspace.

2. General Objective

The **general objective** of this comparative law study (project **EU CYBER VAT**) is to assess the adequacy of the current legal framework at EU and Member State level with regard to combating **cyber-VAT fraud** and to propose solutions to make it more effective and efficient at EU and Member State level. Using the **method of comparative law research**, the project will investigate whether the European criminal law framework for VAT fraud under the **PIF Directive, its implementation by Member States, and national criminal law provisions** can provide a sufficient level of legal protection against the intersection of VAT fraud and cybercrime. As these are **cross-border and particularly serious crimes**, the degree of harmonisation between national rules must always be monitored and ensured.

3. Specific Objectives

The general objective of the project can be divided into the following **3 specific objectives (SO)**:

To provide an analysis of cyber-VAT frauds in the European Union from an empirical criminological point of view, with special attention to the modus operandi as well as the characteristics of the actors involved. The new threats related to the digitalization of tax transactions will be assessed from a criminological perspective, in order to provide a basis for evaluating the adequacy of measures against cyber-VAT fraud in the EU and activities to detect and investigate cyber-VAT fraud by tax and law enforcement authorities;

To provide an account of the transposition of EU criminal law into national legislations to specifically prevent and combat cyber-VAT fraud and an account of the differences between the relevant national legislations of the Member States as well as national best practices;

To elaborate, from the dual perspective of substantive criminal law and criminal procedure, recommendations and proposals to improve the EU regulation and the national anti-fraud strategies (NAFS) against cyber-VAT fraud in order to address the new threats to the financial interests of the European Union in the context of the digital age. This will take particular account of MTIC in the digital marketplace, exploring the possibility of introducing forms of service provider accountability to prevent cyber-VAT fraud. It will also promote a higher level of harmonisation in the regulation of cross-

3. Terminology Clarification

For the purposes of this Questionnaire, for **Cyber VAT fraud** we mean:

"Cyber VAT fraud involves the use of technology to facilitate the overall criminal activity or to assist it in one or more of its stages/phases. The use of technology in one or more stages/phases may include the creation of shell companies using forged documents or identities, the conduct of online transactions and the sale of online goods, including digital goods".

4. Support

Should you have any inquiries, please feel free to contact us

Contacts: cssc@unitn.it

EU CYBER VAT Questionnaire

Member State: _____

Section 1 – Criminal law on VAT Fraud

In this section, we will examine the legal framework of VAT fraud (all types of VAT fraud, not just digital) in the national criminal law of your country, also with regard to Directive (EU) 2017/1371, the so-called PIF Directive.

1. Does your country's national legislation on VAT fraud committed by natural persons comply with Article 3 of the PIF Directive?

*We have carried out a preliminary analysis of EU Member States' national legislation based on desk research and ask you to confirm the findings set out in **Annex 1**. Please use the Annex to: a) confirm or deny the reported information; b) provide clarification in case of non-confirmation through comments; c) provide us with an English version of the text of the relevant legislation.*

1.1 Which of the following acts fall under your national offence(s) of VAT fraud by natural persons?

[Please check all that apply]

☐ All possible conducts of VAT fraud are covered (free-form)

☐ Only some conducts of VAT fraud are covered

If only some conducts, which one?

☐ In respect of revenue other than revenue arising from VAT own resources:

☐ The use or presentation of false, incorrect or incomplete statements or documents

☐ Non-disclosure of information in violation of a specific obligation

☐ Misapplication of a legally obtained benefit

In respect of revenue arising from VAT own resources:

☐ The use or presentation of false, incorrect or incomplete VAT-related statements or documents

	<input type="checkbox"/> Non-disclosure of VAT-related information in violation of a specific obligation <input type="checkbox"/> The presentation of correct VAT-related statements for the purposes of fraudulently disguising the non-payment or wrongful creation of rights to VAT refunds <input type="checkbox"/> Others (please specify)
1.2 Which acts (1.1) are punishable with regard to the subjective elements of your national criminal offence of VAT fraud?	<input type="checkbox"/> Intentional acts only <input type="checkbox"/> Unintentional acts only <input type="checkbox"/> Both
2. Is your national law in line with Article 7 of the VAT Directive with regard to sanctions for natural persons committing VAT fraud?	<p><i>We have carried out a preliminary analysis of EU Member States' national legislation based on desk research and ask you to confirm the findings set out in Annex 2. Please use the Annex to: a) confirm or deny the reported information; b) provide clarification in case of non-confirmation through comments; c) provide us with an English version of the text of the relevant legislation.</i></p>
3. Does your national law contain an aggravating circumstance for the commission of VAT fraud in the context of organised crime, as provided for in Article 8 of the PIF Directive? <small>[If yes, please send us the relevant text of your national law in English]</small>	<input type="checkbox"/> YES <input type="checkbox"/> NO
4. Is your national law on VAT fraud in relation to the liability of legal persons compliant with Article 6 of the PIF Directive?	<p><i>We have carried out a preliminary analysis of EU Member States' national legislation based on desk research and ask you to confirm the results set out in the Annex 3. Please use the Annexes to: a) confirm or deny the reported information; b) provide clarifications in case of non-confirmation through comments; c) provide us with an English version of the text of the relevant legislation.</i></p>
5. Which of the following sanctions provided for in Article 9 of the PIF Directive in relation to legal	<input type="checkbox"/> criminal fine (please specify the extent);

persons recognized as responsible under Article 6 are provided for in your national law?

[Please check all that apply]

- ☐ non-criminal fine (please specify the extent);
- ☐ exclusion from entitlement to public benefits or aid;
- ☐ temporary or permanent exclusion from public tender procedures;
- ☐ temporary or permanent disqualification from the practice of commercial activities;
- ☐ placing under judicial supervision;
- ☐ judicial winding-up;
- ☐ temporary or permanent closure of establishments which have been used for committing the criminal offence.

Section 2 – Criminal law on Cyber VAT Fraud

In this section, we will examine the legal framework of cyber VAT fraud in the national criminal law of your country.

6. Is cyber VAT fraud punishable under the criminal law of your country?

[If yes, please provide us with the relevant text of your national law in English. Not required if it is the same provision as question 1]

- ☐ No
- ☐ Yes, there is a specific criminal offence of cyber VAT fraud
- ☐ Yes, it is punishable under the criminal offence of VAT fraud (as described in Annex 1)
- ☐ Yes, as an aggravating circumstance of VAT fraud (VAT fraud enabled by the use of technology)
- ☐ Other (please specify)

Section 3 – Investigation and prosecution of VAT fraud and cyber VAT fraud

This section examines the investigative tools and measures to combat VAT fraud and cyber VAT fraud, the legal framework of jurisdiction and limitation period on these criminal offences

7. On which investigative tools/measures law enforcement authorities of your country can rely on for investigating VAT fraud?

[Please name the most effective investigative tools. Please base your answer not only on your personal experience and expertise, but also on case studies or publications and cite the relevant sources]

8. Can these investigative tools/measures also be used effectively in the investigation of cyber VAT fraud? Are there any other specific investigative tools/measures that law enforcement authorities in

your country can rely on when specifically investigating cyber VAT fraud?

[Please base your answer not only on your personal experience and expertise, but also on case studies or publications and cite the relevant sources]

9. How could the national criminal procedure be improved to better combat VAT fraud in your country?

[If applicable, please identify the operational challenges that hinder the effectiveness of authorities in detecting and investigating VAT fraud and explain how the proposed improvements could impact these challenges]

10. How could the national criminal procedure be improved to better combat cyber VAT fraud in your country?

[If applicable, please identify the operational challenges that hinder the effectiveness of authorities in detecting and investigating cyber VAT fraud and explain how the proposed improvements could impact these challenges]

11. When does VAT fraud fall under the jurisdiction of your national legislation?

[Please check all that apply]

- ☐ when the criminal offence is committed in whole or in part within your country's territory
- ☐ when the offender is one of your nationality
- ☐ when the offender is a habitual resident in your territory
- ☐ when the criminal offence is committed for the benefit of a legal person established in your territory
- ☐ when the offender is one of your officials who acts in his or her official duty
- ☐ always when the offender is subject to the Staff Regulations at the time of the criminal offence
- ☐ when the offender is subject to the Staff Regulations at the time of the criminal offence just in specific occasions or when specific conditions are fulfilled (please specify which occasions/conditions)
- ☐ in other occasions (please specify the occasions)

12. If the jurisdiction of your country is based on the fact that the offence of VAT fraud was committed by

- ☐ the condition that the prosecution can be initiated only following a report

<p>one of your citizens, what does your national law require?</p> <p><small>[Please check all that apply]</small></p>	<p>made by the victim in the place where the criminal offence was committed</p> <p><input type="checkbox"/> the condition that the prosecution can be initiated only following a denunciation from the State of the place where the criminal offence was committed</p> <p><input type="checkbox"/> other conditions (please specify)</p> <p><input type="checkbox"/> no conditions at all</p>
<p>13. Does your national legislation provide for a limitation period of at least 5 years for the criminal offence of VAT fraud, as provided for in Article 12 of the PIF Directive?</p> <p><small>[If yes, please send us the corresponding text of your national law in English]</small></p>	<p><input type="checkbox"/> YES</p> <p><input type="checkbox"/> NO</p>
<p>13.1 If not, is a limitation period of at least 3 years provided for (on condition that the period may be interrupted or suspended in the event of specified acts)?</p>	<p><input type="checkbox"/> YES</p> <p><input type="checkbox"/> NO</p>
<p>13.2 In which cases does your national legislation provide that a penalty imposed for VAT fraud can be enforced for at least five years from the date of the final conviction?</p>	<p><input type="checkbox"/> in case of a penalty of more than one year of imprisonment</p> <p><input type="checkbox"/> in case of a penalty of imprisonment for a criminal offence which is punishable by a maximum sanction of at least four years of imprisonment</p> <p><input type="checkbox"/> in both the above cases</p> <p><input type="checkbox"/> in none of the above cases</p> <p><input type="checkbox"/> other cases (please specify)</p>
<p>Section 4 – The role of ICT in the strategy / policy to combat cyber VAT fraud</p> <p>This section examines the role of ICT in the strategy/policy to combat cyber VAT fraud, in particular with regard to fraud prevention and detection.</p>	
<p>14. Which of the following anti-fraud strategies/policies involving ICT are most effective against cyber VAT?</p> <p><small>[Please tick all that apply and explain why]</small></p>	<p><input type="checkbox"/> Collection of data by law enforcement agencies</p> <p><input type="checkbox"/> National plan of cybersecurity (e.g. by updating operating systems, applications and security software to protect against vulnerabilities in institutions' digital archives)</p> <p><input type="checkbox"/> Analysis and the monitoring of transactions (e.g. to detect suspicious activities to detect fraud early)</p>

	<input type="checkbox"/> Cross-border cooperation (e.g. digital systems for the exchange of information) <input type="checkbox"/> Submission of information regarding intra-Community transactions (e.g. e-reporting)
15. Are there specific anti-fraud ICT strategies/policies in your country that are particularly useful against cyber VAT fraud? <small>[If yes, please name the specific anti-fraud ICT strategies/policies and explain to what extent they are particularly useful in combating cyber VAT fraud]</small>	<input type="checkbox"/> YES <input type="checkbox"/> NO
16. <i>The EU has noted (as explained in the final report "VAT in the Digital Age - Volume 1 - Digital Reporting Obligations") that there is a fragmented legal framework and very different systems for e-invoicing and e-reporting in different European Member States.</i> In your opinion, is promoting the introduction of digital reporting obligations that optimize the use of digital technologies, e.g. by introducing some minimum requirements for all EU countries, an effective way to combat VAT and cyber VAT fraud? <small>[If yes, please identify the main critical points in your national VAT reporting rules and the specific aspects that would require improvement (e.g. increasing the frequency of reporting)]</small>	<input type="checkbox"/> YES <input type="checkbox"/> NO
Section 5 – Cyber VAT Fraud in the context of e-commerce <i>This section deals with the implementation of Directive 2020/284 and the MOSS scheme</i>	
17. Is the national law of your country compliant with EU Directive 2020/284 Directive regarding the general obligations of payment service providers?	<input type="checkbox"/> YES <input type="checkbox"/> NO
17.1 If not, is the transposition in progress?	<input type="checkbox"/> YES <input type="checkbox"/> NO
17.2 If the transposition is in progress, what is the expected deadline?	
18. <i>Directive EU 2020/284 introduces new obligations for payment service providers in relation to the recording and reporting of payment information for cross-border payments as part of the European Union's action plan to combat VAT fraud in e-commerce.</i> Were these recording/reporting obligations already provided for in your national legislation?	<input type="checkbox"/> YES <input type="checkbox"/> NO

[If yes, please send us the relevant text of your national legislation in English or in the original language]

18.1 If not, were these recording/reporting obligations introduced with the implementation? ☐ YES
☐ NO

19. What sanctions or consequences (e.g. inclusion in specific lists) does your country provide for in the event of a breach of the provider' obligations?

[Please send us the relevant text of your national legislation in English or in the original language]

20. The VAT Mini One Stop Shop (MOSS) is an optional scheme that allows you to account for VAT, which is normally due in multiple EU countries, in just one EU country. ☐ YES
☐ NO

Has your country introduced the MOSS scheme?

21. In your opinion, how could service providers and payment service providers be more involved in the detection and prevention of criminal offences related to VAT fraud?

Section 6 – Case study

In this section, we ask you to provide us with national case studies so that we can conduct a criminological analysis of the modus operandi and characteristics of the actors involved in cyber VAT fraud in the EU.

22. Please select and submit **emblematic cases of cyber VAT fraud** at the national investigation level.

[The empirical criminological analysis aims to assess the behaviours realised in cyberspace that could harm the financial interests of the EU through VAT evasion, focusing on the modus operandi and characteristics of the actors of cyber VAT fraud in the EU, as well as on the role of technologies in the commission of these crimes. Therefore, we please ask you to select and submit emblematic cases at the level of national investigations.

Please attach to your email together with the questionnaire any materials such as publications, court decisions, etc. that report on interesting case studies providing information on modus operandi and perpetrators of cyber VAT fraud within the EU]

Annex II – National provisions | Compliance to Art. 3 of the Directive (EU) 2017/1371 (Questionnaire Appendix 1)

Member State		Compliance	Legal Reference
Austria	Preliminary analysis of national legislation (desk research)	Yes, because of the provision of a new legislation	Art. 40 I. 129/1958 as amended by I. 62/2019
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Belgium	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Art. 73 and 73nonies VAT Code as amended by l. 9 December of 2019
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Bulgaria	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Art. 255 Bulgarian Criminal Code
	Do you confirm the results of the	Yes/No	Yes/No

	preliminary analysis?		
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Croatia	Preliminary analysis of national legislation (desk research)	No, because of not adequate amendments of pre-existing discipline	Art. 236 and 256 Croatian Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Cyprus	Preliminary analysis of national	Yes, because of the provision of a new legislation	Art. 4 l. 4762/2020 as amended by l. 114/2021

	legislation (desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Czechia	Preliminary analysis of national legislation (desk research)	No, because of not adequate amendments of pre-existing discipline	Art. 260 of Czech Criminal Code

	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Denmark	Preliminary analysis of national legislation (desk research)	No, because Denmark is not legally required to transpose the PIF Directive due to Protocol n. 22 of the TFUE. Denmark is legally bound to PIF Convention.	Art. 289 and 289a Danish Criminal Code
	Do you confirm the results of the	Yes/No	Yes/No

	preliminary analysis?		
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		
Member State		Compliance	Legal Reference
Estonia	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Art. 209 Estonian Criminal Code as amended by I. 5/2019
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		

	Text of the relevant legal provision(s)	
--	---	--

Member State		Compliance	Legal Reference
Finland	Preliminary analysis of national legislation (desk research)	No, because of not adequate amendments of pre-existing discipline	Art. 1, 2 and 4 of section 29 Finnish Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

--	--	--

Member State		Compliance	Legal Reference
France	Preliminary analysis of national legislation (desk research)	No, because the pre-existing discipline is not adequate	Art. 313-1, 313-2, 313-3 and 113-14 French Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

--	--	--

Member State		Compliance	Legal Reference
Germany	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Section 264 German Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Greece	Preliminary analysis of national legislation	No, because of the provision of a new legislation not entirely adequate	Art. 23 I. 103/2020

	(desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Hungary	Preliminary analysis of national legislation (desk research)	No, because the pre-existing discipline is not adequate	Art. 396 Hungarian Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Ireland	Preliminary analysis of national	Yes, because of the amendment of pre-existing discipline	Section 42 I. 50/2001, Criminal Justice (Theft and Fraud Offences) Act as amended by I. 2/2021

	legislation (desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Italy	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Art. 316ter and 640 Italian Criminal Code and Art. 2, 3 and 4 D. lgs. 74/2000 as amended by D. lgs. 75/2020 and D. lgs. 156/2022

	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		
Member State		Compliance	Legal Reference
Latvia	Preliminary analysis of national legislation (desk research)	No, because of the amendment of pre-existing discipline	Art. 218, 218.1 and 219 Latvian Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

--	--	--

Member State		Compliance	Legal Reference
Lithuania	Preliminary analysis of national legislation (desk research)	No, because of the amendment of pre-existing discipline	Art. 182, 207 and 220 Lithuanian Criminal Code as amended by I. XIII-2334 and I. XIV-1925
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

--	--	--

Member State		Compliance	Legal Reference
Luxembourg	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Art. 496-4 and 501 Luxembourgian Criminal Code as amended by l. 12 March 2020
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
--------------	--	------------	-----------------

Malta	Preliminary analysis of national legislation (desk research)	Yes, because of the provision of a new legislation	Art. 2 of L. XVIII/2020 that amended art. 190C Maltese Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Netherlands	Preliminary analysis of national legislation	Yes, because of the amendment of pre-existing discipline	Art. 69 and 69a <i>Algemene wet Inzake Rijksbelastingen</i>

	(desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Poland	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Art. 54 and 56 Polish Tax Criminal Code
	Do you confirm the results of the	Yes/No	Yes/No

	preliminary analysis?		
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Portugal	Preliminary analysis of national legislation (desk research)	No, because of not adequate amendments of pre-existing discipline	Art. 36 and 38 D.I. 28/84 of 20 January 2013 as amended by I. 4/2024
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No

	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Romania	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Art. 9.1 l. 241/2005 as introduced by l. 125/2023
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		

	Text of the relevant legal provision(s)	
--	---	--

Member State		Compliance	Legal Reference
Slovakia	Preliminary analysis of national legislation (desk research)	No, because of not adequate amendments of pre-existing discipline	Art 261 Slovakian Criminal Law as amended by I. 214/2019
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

--	--	--

Member State		Compliance	Legal Reference
Slovenia	Preliminary analysis of national legislation (desk research)	No, because of not adequate amendments of pre-existing discipline	Art. 229 Slovenia Criminal Code as amended by art. 32 I. 186/2021
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

--	--	--

Member State		Compliance	Legal Reference
Spain	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Art. 305 and 306 Spanish Criminal Code as amended by art. 10 <i>Ley organica</i> 1/2019
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Sweden	Preliminary analysis of national	No, because the pre-existing discipline is not adequate	Section 2 I. 69/1971

	legislation (desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Annex III – National provisions | Compliance to Art. 7 of the Directive (EU) 2017/1371 (Questionnaire Appendix 2)

Member State		Compliance	Sanction
Austria	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	1 - 10 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Belgium	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	8 days - 5 years

	Do you confirm the results of the preliminary analysis?	Yes/No
	If no, please specify the amendments	

Member State		Compliance	Sanction
Bulgaria	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	1 - 6 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Croatia	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	6 months - 5 years
	Do you confirm the results of the preliminary analysis?	Yes/No	

	If no, please specify the amendments	
--	--------------------------------------	--

Member State		Compliance	Sanction
Cyprus	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	Up to 7 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Czechia	Preliminary analysis of national legislation (desk research)	No, because the maximum penalty laid down in national law is lower than the minimum standard of the PIF Directive	Up to 3 years
	Do you confirm the		

	results of the preliminary analysis?	Yes/No
	If no, please specify the amendments	

Member State		Compliance	Sanction
Denmark	Preliminary analysis of national legislation (desk research)	<p>Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive.</p> <p>Note that Denmark is not legally required to transpose the PIF Directive due to Protocol n. 22 of the TFUE. Denmark is legally bound to the PIF Convention.</p>	Up to 4 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Estonia	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	Up to 4 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Finland	Preliminary analysis of national legislation (desk research)	No, because the maximum penalty laid down in national law is lower than the minimum standard of the PIF Directive	Up to 2 years
	Do you confirm the results of the preliminary analysis?		

	If no, please specify the amendments	
--	--------------------------------------	--

Member State		Compliance	Sanction
France	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	Equal to 5 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Germany	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	Up to 5 years
	Do you confirm the		

	results of the preliminary analysis?	Yes/No
	If no, please specify the amendments	

Member State		Compliance	Sanction
Greece	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	No less than 10 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Hungary	Preliminary analysis of national legislation	No, because the maximum penalty laid down in national law is lower than the minimum standard of the PIF Directive	Up to 3 years

	(desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Ireland	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	Up to 5 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Italy	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	18 months – 6 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Latvia	Preliminary analysis of national legislation (desk research)	No, because the maximum penalty laid down in national law is lower than the minimum standard of the PIF Directive	Up to 2 years
	Do you confirm the results of the preliminary analysis?	Yes/No	

	If no, please specify the amendments	
--	--------------------------------------	--

Member State		Compliance	Sanction
Lithuania	Preliminary analysis of national legislation (desk research)	No, because the maximum penalty laid down in national law is lower than the minimum standard of the PIF Directive	Up to 3 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Luxembourg	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	4 months - 4 years

	Do you confirm the results of the preliminary analysis?	Yes/No
	If no, please specify the amendments	

Member State		Compliance	Sanction
Malta	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	6 months - 4 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Netherlands	Preliminary analysis of national	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	Up to 4 years / 6 years depending on the conduct

	legislation (desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Poland	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	No maximum is set
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Portugal	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	1 - 5 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Romania	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	7 - 15 years
	Do you confirm the results of the preliminary analysis?	Yes/No	

	If no, please specify the amendments	
--	--------------------------------------	--

Member State		Compliance	Sanction
Slovakia	Preliminary analysis of national legislation (desk research)	No, because the maximum penalty laid down in national law is lower than the minimum standard of the PIF Directive	6 months - 3 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Slovenia	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	3 months - 5 years
	Do you confirm the	Yes/No	

	results of the preliminary analysis?	
	If no, please specify the amendments	

Member State		Compliance	Sanction
Spain	Preliminary analysis of national legislation (desk research)	Yes, because the maximum penalty laid down in national law is higher than the minimum standard of the PIF Directive	1 - 5 years
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Member State		Compliance	Sanction
Sweden	Preliminary analysis of national legislation	No, because the maximum penalty laid down in national law is lower than the minimum standard of the PIF Directive	Up to 2 years

	(desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	
	If no, please specify the amendments		

Annex IV – National provisions | Compliance to Art. 6 of the Directive (EU) 2017/1371 (Questionnaire Appendix 3)

Member State		Compliance	Legal Reference
Austria	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Federal law on the criminal liability of associations (artt. 1, 3, 4, 12)
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
--------------	--	------------	-----------------

Belgium	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Art. 5 Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Bulgaria	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Law on administrative violations and administrative sanctions, (art. 83 rd , first paragraph)
	Do you confirm the results of the	Yes/No	Yes/No

	preliminary analysis?		
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Croatia	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Art. 247 Croatian Criminal Code and Law n. 151/2003 (art. 4, 5, 8)
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		

	Text of the relevant legal provision(s)	
--	---	--

Member State		Compliance	Legal Reference
Cyprus	Preliminary analysis of national legislation (desk research)	Yes, because of the provision of a new legislation	Art. 7 I. 4762/2020 as amended by I. 114/2021
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Czechia	Preliminary analysis of national legislation	Yes, because the legislation was already adequate	Section 7, Law n. 418/2011 about the liability of legal persons

	(desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Denmark	Preliminary analysis of national legislation (desk research)	No, because Denmark is not legally required to transpose the PIF Directive due to Protocol n. 22 of the TFUE. Denmark is legally bound to PIF Convention.	Artt. 25, 26, 27 Danish Criminal Code and Law about VAT art. 81
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No

	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Estonia	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Art. 209 Estonian Criminal Code as amended by I. 519/2019
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Finland	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Section 9 Finnish Criminal Code and Art. 10 Law 2019/368
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
France	Preliminary analysis of national legislation (desk research)	No, because the pre-existing discipline is not adequate	Artt. 121-2, 131-37, 131,39 French Criminal Code
	Do you confirm the	Yes/No	Yes/No

	results of the preliminary analysis?		
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Germany	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Law on Administrative Offenses (artt. 30 and 130)
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		

	Text of the relevant legal provision(s)	
--	---	--

Member State		Compliance	Legal Reference
Greece	Preliminary analysis of national legislation (desk research)	No, because of the provision of a new legislation not entirely adequate	Art. 23 I. 103/2020
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Hungary	Preliminary analysis of	Yes, because the legislation was already adequate	Art. 2 of Law 104/2001

	national legislation (desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Ireland	Preliminary analysis of national legislation (desk research)	Yes, because of the provision of a new article	Section 58 I. 50/2001, Criminal Justice (Theft and Fraud Offences) Act as amended by I. 2/2021
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No

	If no, please specify the amendments		
	Text of the relevant legal provision(s)		
Member State		Compliance	Legal Reference
Italy	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing discipline	Paragraph 1-bis, Art. 25-quinquies decies, D. lgs n. 74/2000 as amended by art. 5 D. lgs. 75/2020
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		

	Text of the relevant legal provision(s)		
Member State		Compliance	Legal Reference
Latvia	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Artt. 70 and 70.1 Latvian Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State	Compliance	Legal Reference
--------------	------------	-----------------

Lithuania	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing article	Art. 20 Lithuanian Criminal Code as amended by I. XIII-2334 and I. XIV-1925
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		
Member State		Compliance	Legal Reference
Luxembourg	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Art. 34 Luxembourgian Criminal Code as amended by I. 12 March 2020
	Do you confirm the results of the	Yes/No	Yes/No

	preliminary analysis?		
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Malta	Preliminary analysis of national legislation (desk research)	Yes, because of the provision of a new legislation	Art. 2 of L. XVIII/2020 that amended art. 190G Maltese Criminal Code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		

	Text of the relevant legal provision(s)	
--	---	--

Member State		Compliance	Legal Reference
Netherlands	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Art. 51 Dutch criminal code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Poland	Preliminary analysis of national legislation	Yes, because the legislation was already adequate	Art.3 l. n. 659/2023 about the Liability of legal persons

	(desk research)		
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Portugal	Preliminary analysis of national legislation (desk research)	No, because of not adequate amendments of pre-existing discipline	Art. 11 Portuguese criminal code
	Do you confirm the	Yes/No	Yes/No

	results of the preliminary analysis?		
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Romania	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Art. 135 Romanian criminal code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		

	Text of the relevant legal provision(s)	
--	---	--

Member State		Compliance	Legal Reference
Slovakia	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Art. 4, Law n. 91/2016 about the liability of legal persons
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State	Compliance	Legal Reference
--------------	------------	-----------------

Slovenia	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing article	Art. 4, Law n. 98/04 about the liability of legal person
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Spain	Preliminary analysis of national legislation (desk research)	Yes, because of the amendment of pre-existing article and the legislation was already adequate	Art. 305 and 306 Spanish Criminal Code as amended by art. 10 <i>Ley organica</i> 1/2019 and art. 310.bis
	Do you confirm the	Yes/No	Yes/No

	results of the preliminary analysis?		
	If no, please specify the amendments		
	Text of the relevant legal provision(s)		

Member State		Compliance	Legal Reference
Sweden	Preliminary analysis of national legislation (desk research)	Yes, because the legislation was already adequate	Section 37, art. 7, Swedish criminal code
	Do you confirm the results of the preliminary analysis?	Yes/No	Yes/No
	If no, please specify the amendments		

	Text of the relevant legal provision(s)	
--	---	--