



Brussels, 12.12.2018
SWD(2018) 488 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

**Proposal for a Council Directive amending Directive 2006/112/EC as regards
introducing certain requirements for payment service providers**

and

**Proposal for a Council Regulation amending Regulation (EU) No 904/2010 as regards
measures to strengthen administrative cooperation in order to combat VAT fraud**

{COM(2018) 812 final} - {COM(2018) 813 final} - {SEC(2018) 495 final} -
{SWD(2018) 487 final}

Contents

<u>LIST OF FIGURES</u>	4
<u>1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT</u>	5
<u>1.1. The modernisation of the VAT system on B2C cross-border supplies</u>	5
<u>1.2. Administrative cooperation</u>	7
<u>1.3. Enforcement</u>	8
<u>2. PROBLEM DEFINITION</u>	9
<u>2.1. E-commerce VAT fraud</u>	9
<u>2.1.1. VAT fraud on cross-border supplies of services</u>	10
<u>2.1.2. VAT fraud on intra-EU distance sales of goods</u>	11
<u>2.1.3. VAT fraud on imports of goods</u>	11
<u>2.2. Size of the problem</u>	12
<u>2.3. Problem tree</u>	15
<u>2.4. What are the problem drivers?</u>	15
<u>2.4.1. No physical presence of the suppliers</u>	15
<u>2.4.2. Relevant VAT information held by third parties</u>	16
<u>2.4.3. Tax administration tools and capacities</u>	17
<u>2.4.4. Other Drivers influencing e-commerce VAT fraud (and addressed by other initiatives)</u>	18
<u>2.5. How will the problem evolve?</u>	18
<u>3. WHY SHOULD THE EU ACT?</u>	18
<u>4. OBJECTIVES: WHAT IS TO BE ACHIEVED?</u>	19
<u>4.1. General objectives</u>	19
<u>4.2. Specific objectives</u>	19
<u>4.3. Operational objectives</u>	20
<u>4.4. Consistency with other EU policies and with the Charter for fundamental rights</u>	20
<u>5. WHAT ARE THE AVAILABLE POLICY OPTIONS?</u>	21
<u>5.1. Measures with a positive impact on reducing the e-commerce VAT loss introduced with the VAT e-commerce package)</u>	21
<u>5.1.1. Abolition of the distance sale thresholds and extension of the MOSS</u>	21
<u>5.1.2. Abolition of the small consignments exemption</u>	21
<u>5.1.3. Import One Stop Shop (IOSS)</u>	21
<u>5.1.4. Deemed supplier</u>	22
<u>5.2. Policy options</u>	22
<u>5.2.1. Payment services and payment service providers</u>	24
<u>5.2.2. Payment data</u>	24
<u>5.2.3. Structure of the policy options</u>	25
<u>5.3. What is the baseline from which options are assessed?</u>	26

5.3.1.	Policy option 1 – Baseline scenario	26
5.4.	Description of the policy options	27
5.4.1.	Policy option 2 (non-regulatory): Investing in administrative capacity and providing EU guideline + standard forms	27
5.4.2.	Policy option 3 (Regulatory option): Collection and exchange of payment data	28
5.5.	Discarded option	31
5.5.1.	VAT split payment	31
5.5.2.	Direct access of Member States' tax authorities to Payment Service Providers' databases	31
6.	WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?	31
6.1.	Methodology	31
6.2.	Analysis of the impacts	31
6.2.1.	Impact on VAT fraud	33
6.2.2.	Impact on distortion of competition	39
6.2.3.	Impact on administrative burden and compliance costs	42
6.2.4.	Sectoral impacts	45
6.2.5.	Impact on terms of trade, employment and environment	46
6.2.6.	Impact in terms of the fundamental right to protection of personal data ...	46
7.	HOW DO THE OPTIONS COMPARE?	48
7.1.	Summary assessment of the impact	48
8.	PREFERRED OPTION	50
8.1.	Identification of the preferred option	50
8.2.	Subsidiarity of the preferred option	50
8.3.	Proportionality of the preferred option	51
8.4.	Impact on SMEs	51
9.	HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?	52
9.1.	Indicators for monitoring and evaluation	52
9.2.	Monitoring structure	52
10.	ANNEXES	53
10.1.	Annex 1: Procedural information	54
10.2.	Annex 2: Consultation synopsis report	56
10.3.	Annex 3: Evaluation of Regulation (EU) 904/2010 for cross-border Business to Consumer online supplies	67
10.4.	Annex 4: Who is affected by the initiative and how?	92
10.5.	Annex 5: Methodology	95
10.6.	Annex 6: Technical feasibility of the options	96
10.7.	Annex 7: Case Study – pricing policy and estimation of potential VAT loss	103
10.8.	Annex 8: Result of the TAXUD 2016 survey on e-commerce compliance strategies in the EU	112

<u>10.9. Annex 9: Payment Services framework in the EU</u>	114
<u>10.10. Annex 10: B2B import VAT fraud</u>	116
<u>10.11. Annex 11: Third countries using payment data as VAT control tool</u>	118
<u>10.12. Annex 12: Visual examples of the regulatory options</u>	119
<u>10.13. Annex 13: Comparison amongst different initiatives in terms of fighting e-commerce VAT fraud</u>	121

GLOSSARY

<i>Term or acronym</i>	<i>Meaning or definition</i>
B2B	Business-to-business.
B2C	Business-to-consumers.
C2C	Consumers-to-consumers
EBA	European Banking Authority
E-commerce	The sale or purchase of goods or services through electronic transactions conducted via the internet or other computer-mediated (online communication) networks ¹
E-commerce VAT fraud	VAT fraud on B2C cross-border supplies of goods and services. It covers intra-EU distance sales of goods, imports of goods, and cross-border supplies of services (from suppliers established in one Member State or in a third country)
GDPR	General Data Protection Regulation
IOSS	Import One Stop Shop
MLCs	Multilateral controls
MOSS	Mini One Stop Shop
MSC	Member State of Consumption
MSE	Member State of Establishment
MTIC Fraud	Missing Trader Intra-Community
PSD2	Payment Service Directive 2
PSP	Payment Service Providers
SEPA	Single euro payment area
TBE	Telecommunications, broadcasting and electronic services
VAT	Value-Added Tax
VC	Virtual Currencies

¹ Eurostat glossary: <http://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:E-commerce>

LIST OF FIGURES

Figure 1: Turnover from B2C and B2BG (Businesses and Governments) web sales, percentage share on total, non-financial enterprises, EU-28, 2017	12
Figure 2: Sectoral distribution of e-commerce, 2017	12
Figure 3: Problem tree	14
Figure 4: Link between drivers, options (non-regulatory and regulatory) and specific objective	25
Figure 5: Respondents to the public consultation (number)	57
Figure 6: Country of residence of the respondents to the public consultation (number) .	57
Figure 7: Perception of the negative impact of VAT fraud in e-commerce	59
Figure 8: Proportionality of the initiative	61
Figure 9: Subsidiarity of the initiative	61
Figure 10: Public consultation: Comparison of policy options	61
Figure 11: Public consultation: Preferred technical choices	62
Figure 12: Public consultation: Exchange of data must not reveal the identity of the customer (buyer)	62
Figure 13: Tax authorities: evaluation of the administrative cooperation tools	63
Figure 14: Regulation (EU) 904/2010: intervention logic	69
Figure 15: Tax authorities: perceived effectiveness of the administrative cooperation tools	79
Figure 16: Positive and negative perception on the effectiveness of different administrative cooperation tools	80
Figure 17: Tax authorities: perception on the administrative cooperation tools	83
Figure 18 - Public consultation: Public perception of the EU added value	87
Figure 19: Tax authorities: perception of the EU added value	87
Figure 20: Public consultation: perception on the e-commerce VAT fraud problem	88
Figure 21: Distributed application exchange of info	118
Figure 22: Central repository of data	119

LIST OF TABLES

Table 1: Main modalities of fraud on B2C cross-border transactions	9
Table 2: Tax administrations' estimates of annual VAT losses, by type, EUR million ...	11
Table 3 Fraud levels: net impacts over baseline, by option	37
Table 4: Total Member State + EU Commission costs for payments data IT infrastructure (EUR million; rounded)	42
Table 5 Audits for which the use of payments data was important	43
Table 6: Summary analysis of impacts	47
Table 7: Evaluation matrix	74
Table 8: Simplified example of payment data transmitted to a Member State from the Payment Service Providers established in that Member State	118
Table 9: Comparison amongst different initiatives in terms of fighting e-commerce VAT fraud	120

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

Business-to-consumer (B2C) cross-border supplies of goods and services are facilitated by the rapid growing of the e-commerce², which offers more opportunities to both businesses and consumers. However, the same opportunities are also exploited by dishonest traders – located both inside and outside the EU - to gain an unfair market advantage by not fulfilling the VAT obligations. As private consumers change purchase habits and suppliers adapt their business models, tax authorities are facing new challenges in coping with B2C cross-border VAT fraud (hereinafter e-commerce VAT fraud).

The initiative supported by this impact assessment complements the current VAT regulatory framework as recently modified by the VAT e-commerce Directive³ in the framework of the Commission Digital Single Market Strategy⁴. In December 2017, when the VAT e-commerce Directive was adopted, the Council stressed the need to strengthen cooperation between Member States in order to tackle VAT fraud⁵. The options taken into account in this initiative have been drafted after consultation with several Member States and business representatives (including payment service providers and other online platforms) in the framework of the VAT forum⁶.

In particular this impact assessment identifies areas where the administrative cooperation framework can be improved to better tackle fraud and restore fair competition.

An evaluation of Council Regulation (EU) 904/2010, on administrative cooperation and fighting fraud in the field of VAT is in annex of this report⁷. The evaluation, based on the answers of the Member States' tax administrations to a targeted consultation and on an open consultation, shows that administrative cooperation is crucial to combat e-commerce VAT fraud, but the evolution of the business models and fraud patterns in the e-commerce pose new challenges to Member States that must be addressed with new administrative cooperation tools⁸.

1.1. The modernisation of the VAT system on B2C cross-border supplies

The general rule applying to cross-border B2C supplies of goods and services as laid down in the VAT Directive⁹ is the so-called “destination principle”: taxation in the Member State of consumption. In the EU VAT system, when applying the destination principle, in general¹⁰, the suppliers of goods and services should register in the Member

² In 2016, the e-commerce turnover increased by 15% in Europe and it was expected to reach over EUR 600 billion in 2017. Source Ecommerce Europe "European B2C E-commerce Report 2017".

³ Council Directive (EU) 2017/2455 of 5 December 2017 amending Directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations for supplies of services and distance sales of goods, OJ L 348, 29.12.2017, p. 7

⁴ COM(2017) 228 final of 10/5/2017, Implementation of the Digital Single Market Strategy, see: <https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review>

⁵ Council of the European Union, 14769/1/17 REV 1, 30 November 2017

⁶ Commission Decision 2012/C 198/05 of 3 July 2012 setting up the EU VAT Forum, OJ C198 of 6 July 2012

⁷ The evaluation was carried out on the basis of a public consultation, a targeted consultation with the main stakeholders concerned, and desk research. The evaluation was also built up on the findings of a more comprehensive evaluation of Regulation (EU) 904/2010 that was carried out in 2017. See Annex 3 "Evaluation"

⁸ See Annex 3 "Evaluation of Regulation (EU) 904/2010 for cross-border Business to Consumer online supplies"

⁹ Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax *OJ L 347, 11.12.2006, p. 1*

¹⁰ Note that there are several exceptions due to the nature of the goods or service traded. For details, see : http://ec.europa.eu/taxation_customs/business/vat/eu-vat-rules-topic/where-tax_en

State of destination where the customer is established or where the goods arrive and, thus, comply with the appropriate set of rules in each different Member State. The destination principle applies also to B2C supplies from non-EU countries: the suppliers are generally liable for the VAT of the Member State where the customer resides. This represents a significant complication for businesses both in the EU¹¹ and in third countries; the compliance burden is heavy enough to make it plausible that part of the VAT loss generated by non-declaration is due to businesses not understanding their tax obligations or finding them too burdensome.

This problem has been addressed by a recent series of initiatives introducing new rules that make it easier for online businesses (both from inside or outside the EU) to comply with VAT obligations and to facilitate the collection of VAT for tax administrations.

In 2015, a simplified electronic and registration system called Mini One Stop Shop (MOSS)¹² entered into force in the field of telecommunication, broadcasting and electronically supplied services (TBE). The suppliers that opt for the MOSS can fulfil all the VAT obligations (identification, declaration, payments) relating to the TBE supplies in one single Member State of their choice (instead of having to register in all the Member States of consumption)¹³. The MOSS represents a simplification for the businesses in the TBE sector and has been a success for the EU Member States in terms of VAT collection¹⁴. The recently adopted legislation modernising the VAT system on B2C cross-border supplies (hereinafter the VAT e-commerce package) will extend the MOSS to all supplies of services and goods intra-EU and from outside the EU (as from 2021)¹⁵.

Furthermore, the VAT e-commerce Directive abolished the thresholds on distance sales¹⁶ and the threshold on small consignment exemptions on importation¹⁷ that add complications for businesses and are exploited by fraudsters to avoid the payment of the due VAT (See section 2.1.2 and section 2.1.3).

Finally, a new provision in the VAT Directive¹⁸ will make online market places, platforms and portals "deemed suppliers" for the sales of goods facilitated through their electronic interfaces. They will be deemed to have received and supplied those goods themselves for a) distance sales of goods imported from third territories or third countries not exceeding the value of EUR 150¹⁹ and b) the B2C supplies of goods which are

¹¹See: <https://www.ecommerce-europe.eu/app/uploads/2016/07/survey-barriers-to-growth-ecommerce-europe-2015-1.pdf>

¹²See: https://ec.europa.eu/taxation_customs/business/vat/telecommunications-broadcasting-electronic-services_en#current_rules

¹³ The Member State of identification will then redistribute the collected VAT to all the Member States of consumption

¹⁴The MOSS led to a collection of EUR 3 billion of VAT in 2015 and EUR 3.2 billion in 2016. 88% was collected under the Union scheme. Source: Commission services

¹⁵See: https://ec.europa.eu/taxation_customs/business/vat/digital-single-market-modernising-vat-cross-border-ecommerce_en

¹⁶ Member States must apply a threshold of either EUR 35 000 or EUR 100 000, Article 34 of Directive 2006/112/EC: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:347:0001:0118:en:PDF>

¹⁷ Article 23 of Council Directive 2009/132/EC of 19 October 2009 provides that goods of a total value not exceeding EUR 10 shall be exempt on import. Member States may grant exemption for imported goods of a total value of more than EUR 10, but not exceeding EUR 22 and can exclude goods imported on mail order (including e-commerce channels). The exemption excludes excisable goods

¹⁸ New Article 14a of the VAT Directive as amended by Council Directive (EU) 2017/2455 of 5 December 2017 amending Directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations for supplies of services and distance sales of goods, OJ L 348, 29.12.2017, p. 7

¹⁹ Above the value of EUR 150 a full customs declaration is required. The Import One Stop Shop system can only be applied for goods sold to private consumers in the EU and being imported from third countries

already in the EU (i.e. in fulfilment centers) by non-EU established taxable persons facilitated through these platforms. This measure also represents a simplification for the tax authorities of the Member States that will be able to collect the VAT due on certain B2C supplies of goods and imports directly from a single taxable person (the deemed supplier) and not from numerous suppliers not established in the EU. However, under this provision, the tax authorities will not be able to detect or control fraudulent transactions. Also under the deemed supplier provision Member States will have the same need they currently have to check that all the transactions are declared, or correctly declared.

The recently adopted measures are designed to reduce the administrative burdens, facilitate compliance and making the VAT system more fraud proof by abolishing the thresholds on distance sales and on the exemption for small consignments. While they modernised the VAT system in order to make it easier for businesses trading cross-border to comply with their obligations and for tax authorities to collect VAT, no adequate and new administrative cooperation instruments had been introduced to address the specificities of the e-commerce VAT fraud.

The consultation supporting this impact assessment, showed that the magnitude of the problem is still unknown by some of the Member States because of the lack of data at disposal of tax administrations²⁰. However, recent fraud cases in the field of e-commerce raised now the need to provide tax authorities with new tools addressing the specific problem (see section 2).

1.2. Administrative cooperation

As stressed by the experts of tax authorities and businesses in the framework of the EU VAT Forum²¹, the traditional cooperation to combat VAT fraud is between tax authorities and is based on records held by the businesses directly involved in the transaction chain. In the cross-border B2C supplies, this information may not be directly available and thus the "traditional" cooperation between tax authorities is not enough²².

In fact, the evaluation showed that the current administrative cooperation tools are used to a very limited extent (only five Member States reported to have received spontaneous information on e-commerce VAT fraud²³ and half of the respondent Member States reported difficulties in receiving information on request from the other Member States on e-commerce VAT fraud). The number of requests for information to other Member States on e-commerce VAT fraud is still very low (in 2017 only 319 requests) compared to the total number of requests for information processed by the Member States in the field of VAT (in 2017 more than 45.000). The reason of these difficulties lies in the lack of third party data, as pointed out by the experts of the e-commerce sub group of the VAT forum.

The Commission proposal recently agreed by the Council²⁴ amending Council Regulation (EU) No 904/2010 as regards measures to strengthen administrative

up to a value of EUR 150. Therefore, the deeming provision is limited to importation of such goods when their value remains under EUR 150.

²⁰ See Annex 2, "Consultation synopsis report".

²¹ Commission Decision 2012/C 198/05 of 3 July 2012 setting up the EU VAT Forum, OJ C198 of 6 July 2012

²² Consolidated report on Cooperation between Member States and Businesses in the field of e-Commerce/modern commerce, p. 5. See: https://ec.europa.eu/taxation_customs/business/vat/vat-reports-published_en

²³ See Annex 3, "Evaluation of Regulation (EU) 904/2010 for cross-border Business to Consumer online supplies"

²⁴ <http://www.consilium.europa.eu/media/35761/st10203-en18.pdf>

cooperation in the field of VAT²⁵ will provide for new tools on administrative cooperation between tax administrations mainly addressed to fight the so-called “carousel fraud” (carried out on business-to-business B2B transactions), the fraud involving the margin scheme applicable to second-hand cars and the fraud exploiting specific customs regimes applicable to imports carried out by taxable persons (again on B2B transactions). In addition, Eurofisc officials will be entitled to exchange relevant information on VAT fraud cases with Europol and the European Anti-Fraud Office (OLAF). However, the above proposal will not affect VAT fraud on cross-border B2C transactions. The peculiarity of the B2C e-commerce schemes was mentioned in the Commission VAT Action plan²⁶. In particular, the Commission pledged to address VAT fraud in the electronic commerce sector by means of specific anti-fraud tools for tax administrations, in cooperation with third parties that facilitate the B2C cross border supplies of goods and services²⁷. Therefore, this initiative is to be seen as complementary to the above mentioned amendments to Regulation (EU) 904/2010 to strengthen administrative cooperation in the field of VAT, by giving tax authorities the sources of information they are currently unavailable to them, as pointed out by the experts of the e-commerce sub group of the VAT forum.

1.3. Enforcement

The detection of fraudsters established in a state different from the one of consumption is only a first step for tax administrations. Making the fraudsters comply with VAT obligations (i.e. VAT registration, VAT declaration and VAT payment) is a subsequent step to be addressed through enforcement measures, which are not part of this impact assessment and of the future proposal. Still, as a matter of consistency, it is worth mentioning enforcement initiatives related to this anti-fraud initiative. When the remote suppliers are established in the EU, the tax authorities of the EU Member States can use the European mutual assistance framework²⁸ to notify documents and apply recovery measures. However, when the remote suppliers are established outside the EU the enforcement may be more difficult. Member States can activate international cooperation under bilateral agreements or the Council of Europe/OECD multilateral Convention on administrative cooperation on tax matters²⁹. Nevertheless, even in this case, some countries apply the reservation of the Convention excluding VAT (and other consumption taxes) from its scope³⁰.

This problem is internationally recognised and the OECD recommends strengthening the international administrative cooperation on VAT or sales tax to address the challenges of collecting VAT from non-resident suppliers, particularly in B2C trade³¹. A step forward in this respect is the Agreement between the European Union and Norway in the field of

²⁵ COM(2017)706 final

²⁶COM(2016) 148 final, point 3.4

²⁷Point 6 of 20 measures to tackle the VAT gap, annex to the VAT Action plan

²⁸ Council Directive 2010/24/EU of 16 March 2010 OJ L 84, 31.3.2010, p. 1.

²⁹See: <http://www.oecd.org/ctp/exchange-of-tax-information/convention-on-mutual-administrative-assistance-in-tax-matters.htm>

³⁰See: <https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/127/declarations>

³¹ 2017 OECD’s International VAT/GST Guidelines and the BEPS Report on “Addressing the Tax Challenges of the Digital Economy”, see: <http://www.oecd.org/tax/international-vat-gst-guidelines-9789264271401-en.htm>

VAT administrative cooperation (concluded in June 2018³²) that also includes specific instruments for the recovery of VAT claims.

The present initiative will give Member States the evidence to detect fraudsters in third countries as a first step to activate international cooperation or to open an international dialogue to reinforce administrative cooperation tools.

2. PROBLEM DEFINITION

2.1. E-commerce VAT fraud

VAT non-compliance can be essentially ascribed to two main categories of taxpayers: suppliers (basically small and medium enterprises) not fulfilling VAT obligations because of the complexity of the system and suppliers not fulfilling the VAT obligations to intentionally gain illicit market advantages. Tax simplification policies can reduce the type of non-compliance deriving from administrative burden avoidance, but cannot address intentional non-compliance (fraud). While the initiatives described in point 1.1 addressed the first problem, this initiative addresses VAT fraud only.

In particular, the problem at stake refers to VAT fraud on cross-border suppliers to final consumers (B2C). Also a taxable person can buy goods and services online from another taxable person (B2B). However, in this case the tax administration of the Member State of Consumption (MSC), where the VAT is to be paid, can in principle trace back the transaction chain through the records held by the taxable person acquiring the goods and services in its own jurisdiction, and subject to record-keeping obligations³³. This is not the case for cross-border B2C supplies where the consumer has no record-keeping obligations. Furthermore, consumers, unlike taxable persons, do not recover the VAT paid on their purchases. Therefore, in a B2C sale, the buyer has a clear economic incentive to avoid the tax. Unscrupulous suppliers face the same incentive because avoiding VAT will allow them to set prices lower and undercut the competition from law-abiding businesses. Finally, it should be noted that VAT fraud on B2B transactions (in particular Missing Traders and carousel fraud) is tackled already by the recently adopted amendments to Regulation (EU) 904/2010 (see section 1.2).

When dealing with B2C cross-border supplies, the following VAT fraud patterns have been identified (domestic transactions are out of scope):

- The supplier might not register at all for VAT (non-registration);
- The supplier might register but not declare or pay VAT (in total or partially);
- The supplier might under-declare the value of the goods;
- Upon importation, the supplier might mis-describe the good on the package (i.e. as sample, gift...) or, under-declare its value (for example, to profit from the VAT exemption of packages under a value of 10/22 euros);
- The supplier might submit his VAT declaration and pay VAT in the wrong Member State (for example, to profit from a lower VAT rate).

The above-mentioned cases can apply to three types of cross-border B2C transactions:

³²See:

http://dsms.consilium.europa.eu/952/Actions/Newsletter.aspx?messageid=22950&customerid=52749&password=enc_665135434B47373431325650_enc/

³³ Council Regulation (EU) No 904/2010 already provides Member States with specific tools to fight B2B schemes, and new specific measures have been submitted for adoption to the Council. See Annex 10

- Cross-border supplies of services in the cases where the destination principle is of application (both intra-EU and from suppliers located outside the EU³⁴);
- Intra-EU distance sales of goods;
- Imports of goods from non-EU countries.

Table 1: Main modalities of fraud on B2C cross-border transactions

	No VAT registration	No VAT declaration and payment	Under-declaration	Mis-description of the import	VAT declaration in the wrong place
Cross-border supplies of services	✓	✓			
Intra-EU distance selling of goods	✓	✓			✓
Imports of goods from non-EU sellers		✓	✓	✓	

E-commerce business models are multiple and keep evolving. However, they all have something in common: goods and services can be ordered and paid online from the final consumers to the suppliers and no physical presence of the seller is necessary in the Member State of consumption (MSC). VAT e-commerce fraudsters exploit the Internet and its facilities to get easily in contact with consumers abroad and sell services or goods without fulfilling VAT obligations. This allows them to offer lower prices, gain illicit market advantages and remain anonymous *vis-à-vis* the tax authorities. The contacts between suppliers and potential clients are facilitated by online intermediaries such as online market places, online auction sites or search engines that can aggregate the best online suppliers by lower price per category of product, best rank by clients' feedback, etc.

In the section below, examples of VAT fraud are presented to describe the risks posed to VAT collection in e-commerce and the need to provide tax authorities with new tools to detect these types of VAT fraud.

2.1.1. VAT fraud on cross-border supplies of services

TBE services supplied cross-border to final consumers are taxable in the Member State of consumption. Businesses in or outside the EU can fulfil their VAT obligations on cross-border sales of TBE services to European consumers either through the MOSS or by registering, declaring and paying VAT in every MSC³⁵.

However, various instances of VAT fraud have been reported: there are businesses providing TBE services that do not register in the MSC nor identify in the MOSS and, thus, do not declare and pay VAT on their supplies. There is evidence of this kind of fraud in the markets for online television³⁶ and digital games³⁷.

In the first case, websites advertise and offer TV programs to customers in the EU at extremely low prices compared to the normal market price. The client has to order a media box, connect it to the internet and set it to start watching the TV services under a periodic subscription. The web shops often have domain addresses located in third countries, while the real businesses behind them could be placed either inside or outside

³⁴ In B2C supplies of services, the destination principle is not applied universally but depends on the nature of the service. For example, for consultancy services or for transactions related to real estate the principle is not applied. However, the destination principle is applied for example to the sale of telecommunication, broadcasting and electronic services, which represent an important share of cross-border B2C flows.

³⁵ See section 1.1

³⁶ The amount of illegal TV broadcasting in Latvia in 2015, source: www.parlegalusaturu.lv

³⁷ See Annex 2, Consultation synopsis report, section 3.1

the EU. The television content is easily delivered through the Internet Protocol Television (IPTV) using the Internet, instead of being delivered through traditional terrestrial, satellite signal and cable television formats. This fraud was documented by EUROPOL and the European Union Intellectual Property Office³⁸ and by the Nordic Content Protection (NCP) in the latest Report about illegal distribution and sales of access to television broadcasts³⁹. An annual estimated loss in sales of EUR 436 million for IPTV distributors in Denmark, Finland and Sweden alone (having together less than 10% of the total IPTV EU market in terms of revenues)⁴⁰, results in approximately EUR 103 million of potential VAT loss calculated using the standard rates.

Digital games associations have also reported VAT fraud. The mechanism is again very simple: big actors in the European market established both inside and outside the EU, without VAT identification (and without declaring or paying VAT), sell games in the European market with lower prices than their legitimate counterparts⁴¹.

Both cases of fraud also raise copyright issues, which are not under the scope of this impact assessment report.

2.1.2. VAT fraud on intra-EU distance sales of goods

When a European supplier sells goods to final consumers in other Member States, it should register, declare and pay VAT in that Member State (MSC) when its annual supplies in that MSC exceed a given thresholds⁴². If the threshold is not exceeded, the place of supply remains in the Member State of the supplier. The distance selling thresholds had been introduced to avoid small businesses supplying abroad to register in each MSC for every supply and deal with different tax authorities, national legislations and procedures (which represents a burden for these businesses).

Distance selling fraudsters exploit the internet to get easily in contact with clients in other Member States and supply abroad avoiding VAT registration (and thus declaration and payment) in the MSC even when the threshold is exceeded. In such a case, the VAT is paid in the wrong place – the Member State of establishment (MSE), where, usually, the VAT rate is lower. For example⁴³, an Irish trader could make supplies of children clothes to customers in Denmark charging the 0% rate applicable in Ireland. The corresponding rate of VAT in Denmark is 25%.

The distance sales' fraudsters can also remain entirely in the black market by registering (and thus declaring and paying VAT) neither in the MSE nor in the MSC.

There has been increasing evidence of the abuse of distance selling driven by e-commerce that is of great concern for the Member States. The Finnish tax administration alone, in 2016, assessed an amount of EUR 20 million of non-declared VAT by distances sellers.

³⁸ EUROPOL and European Union Intellectual Property Office: 2017 Situation Report on Counterfeiting and Piracy in the European Union available at www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union

³⁹ Trend Report 2017, Nordic Content Protection available at: www.ncprotection.com/wp-content/uploads/2017/03/Trend-Report-2017.pdf

⁴⁰ See: www.ofcom.org.uk/data/assets/pdf_file/0027/95661/ICMR-2016-4.pdf

⁴¹ See: http://www.lemonde.fr/pixels/article/2018/03/22/jeu-video-la-contestation-sociale-s-internationalise_5274955_4408996.html

⁴² Member States must apply a threshold of either EUR 35 000 or EUR 100 000, Article 34 of Directive 2006/112/EC: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:347:0001:0118:en:PDF>

⁴³ SWD(2016)379 final of 1.12.2016 Impact Assessment accompanying the document "Proposal for a Council Directive, a Council Implementing Regulation and a Council Regulation on Modernising VAT for cross-border B2C e-Commerce"

2.1.3. VAT fraud on imports of goods

VAT on imports must be paid applying the right VAT rate (depending on the category of goods and on the Member State of importation) to the value of the goods. VAT fraud on importation can be committed by:

- under-declaring the value of the goods (to unduly benefit from either the small consignment exemption⁴⁴ or just a lower amount of VAT);
- mis-describing the import as a low-value sample⁴⁵ (to benefit from the exemption) or
- pretending to make a C2C transaction (instead of B2C), thus avoiding the VAT on importation.

Similarly to the previous examples, the order and the payment are made online and often the VAT number of the supplier is displayed neither in the web shop nor on the import and transport documents (or it does not exist) and the amount of VAT does not appear under the total price. There is multiple documented evidence of such VAT fraud⁴⁶.

2.2. Size of the problem

VAT is a major source of tax revenue for the Member States⁴⁷ and contributes to the own resources of the European Union. However, measuring the scale of the VAT loss on B2C cross-border supplies is very challenging. Most tax authorities lack the tools and the sources of information to quantify the evidence on the level of e-commerce VAT fraud. However, they consider the level of non-compliance to be significant⁴⁸. In the targeted consultation, only three tax authorities⁴⁹ provided rough estimates on the VAT loss splitting in B2C intra-EU supplies of goods, B2C intra-EU supplies of services and imports of goods in 2015, 2016 and 2017.

Table 2: Tax administrations' estimates of annual VAT losses, by type, EUR million

Austria	B2C Intra-EU supplies of goods (2017)	160
Finland	B2C Intra-EU supplies of goods (2017)	5
Croatia	B2C intra-EU supply of services	1
Finland	Imports (2017)	20
Austria	Imports (2017)	76

The scale of VAT losses undoubtedly differs substantially from one Member State to the other because the rate of penetration of e-commerce is highly uneven. Supply side statistics show that the market for e-commerce is up to seven times more developed in certain Member States over others (see Figure 1); while demand-side statistics, if they

⁴⁴ Article 23 of Council Directive 2009/132/EC of 19 October 2009 provides that goods of a total value not exceeding EUR 10 shall be exempt on import. Member States may grant exemption for imported goods of a total value of more than EUR 10, but not exceeding EUR 22 and can exclude goods imported on mail order (including e-commerce channels). The exemption excludes excisable goods.

⁴⁵ Council Directive 2009/132/EC of 19 October 2009 determining the scope of Article 143(b) and (c) of Directive 2006/112/EC as regards exemption from value added tax on the final importation of certain goods

⁴⁶ Full evidence on Retailers Against VAT Abuse Schemes (RAVAS) and VATfraud.org.

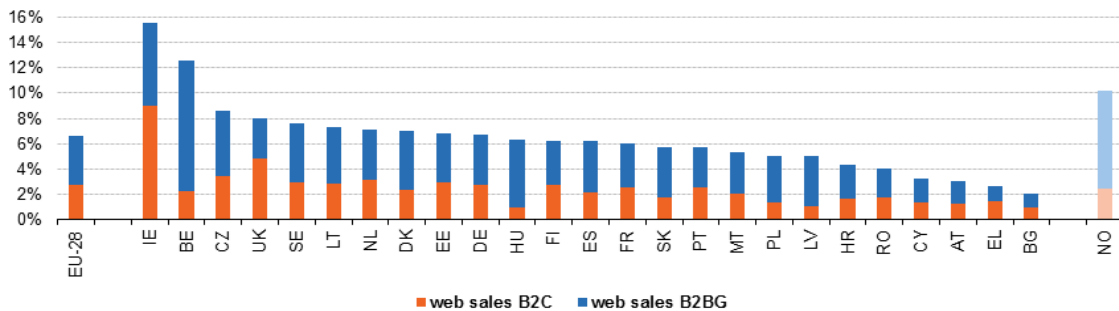
⁴⁷ See: http://ec.europa.eu/eurostat/statistics-explained/index.php/Tax_revenue_statistics

⁴⁸ Deloitte study on VAT Aspects of cross-border e-commerce - Options for modernisation, Lot 1, p. 62

⁴⁹ See Annex 2, Consultation synopsis report, section 3.2

existed, would most probably show a more even picture⁵⁰, it remains likely that the share of VAT losses are quite highly concentrated.

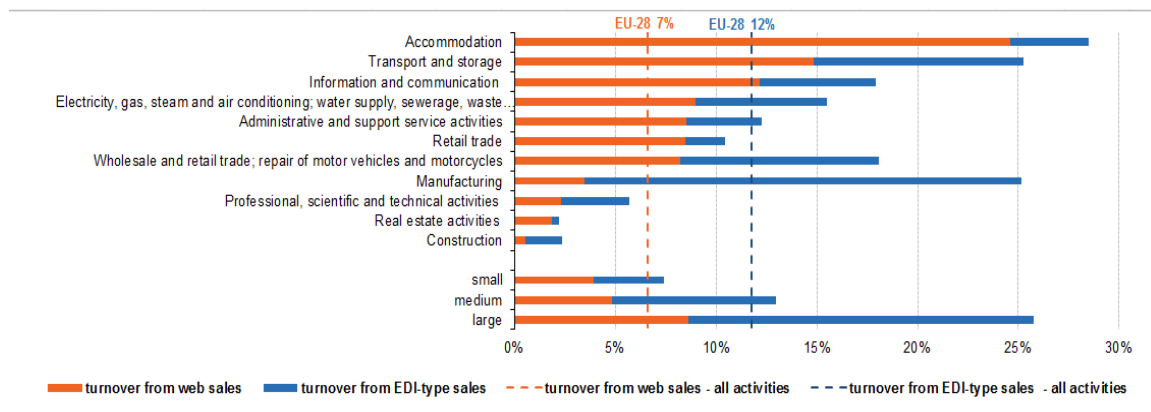
Figure 1: Turnover from B2C and B2BG (Businesses and Governments) web sales, percentage share on total, non-financial enterprises, EU-28, 2017



Source: Eurostat

Statistics on the proportion of e-commerce sales in the turnover of EU businesses show, as of 2017, for the EU28, 7% of overall turnover are constituted of web sales (up from 4% five years earlier), and that this proportion increases along with the size of the business (from 4% for enterprises between 10 and 49 employees to 9% for large enterprises). The B2C portion of web sales is 41%, equivalent to 3% of turnover for EU businesses as a whole. Within this general picture, however, there is a fairly strong differentiation in the level of development of web sales depending on the Member States. The penetration rate of web sales is not merely a function of GDP per capita, but depends on a host of idiosyncratic factors; for example, in Austria the rate is less than one third of Lithuania's. The diffusion of e-commerce also differs significantly by economic sector. The highest proportion of e-commerce is found in accommodation and transport, on account of the popularity of web sales for travel services, whereas e-commerce understandably accounts for only a negligible share of turnover in construction (see Figure 2)⁵¹.

Figure 2: Sectoral distribution of e-commerce, 2017



Source: Eurostat

⁵⁰ The share of individuals having used internet for purchases in the last year is somewhat less polarised: the lowest value, for Romania, is 26%, the highest is for UK at 86%. However, this represents the share of the population having made purchases online, and not the share of turnover, which is the relevant metric to assess potential VAT losses.

⁵¹ Note that EDI-type sales relate to B2B e-commerce. Web sales in contrast can refer both to B2B and to B2C.

Estimates of VAT loss on imports and B2C intra-EU supplies of goods at EU level have been made in the framework of the Commission proposal on "modernising VAT for cross-border B2C e-Commerce": EU Member States are estimated conservatively to be losing between EUR 2.6 and 3.8 billion annually in missing VAT on B2C cross-border supplies of goods (intra-EU and imports)⁵². In addition, the incomplete levying of VAT on postal shipments into the EU is estimated to cause a loss the Member States' income of up to EUR 1.05 billion per year⁵³. The sellers that do not fulfil the VAT obligations gain a market advantage over the legitimate businesses. The impact on businesses has been estimated for the UK. HMRC's estimate of the extent of online VAT fraud for imported goods of £1 billion to £1.5 billion corresponds to £6 billion to £9 billion in lost gross sales revenue for VAT-compliant companies in 2015-16⁵⁴. Applying the same methodology, the VAT loss estimation at EU level would result in EUR 13 to 19 billion of net sales equivalent⁵⁵ to the detriment of legitimate businesses.

The loss to the Member States' and the Union's budget and the negative impact on legitimate businesses' sales are bound to get worse with the steady growth of the e-commerce.

In particular, the MOSS and its extension to all supplies of services and goods intra-EU and from outside the EU (from 2021) are optional systems for compliant businesses. If not accompanied by anti-fraud measures the fraudsters will have no "incentives" in changing attitude and start complying. In other words the full success of the compliance measures in the field of e-commerce also depends on the effectiveness of anti-fraud measures to be developed in parallel.

Finally, it is important to note that VAT revenues are used by the Member States to finance public services and infrastructures for their own citizens. Therefore, also the European citizens are suffering from the VAT fraud. Wide concern about e-commerce VAT fraud resulted also from the public consultation where up to 92% of the respondents considered that the e-commerce VAT fraud is damaging public revenues, consumers and, finally, compliant businesses.

⁵² Deloitte study on VAT Aspects of cross-border e-commerce - Options for modernisation, Lot 1, p. 65

⁵³ SWD(2016)379 final of 1.12.2016 Impact Assessment accompanying the document "Proposal for a Council Directive, a Council Implementing Regulation and a Council Regulation on Modernising VAT for cross-border B2C e-Commerce", p. 14

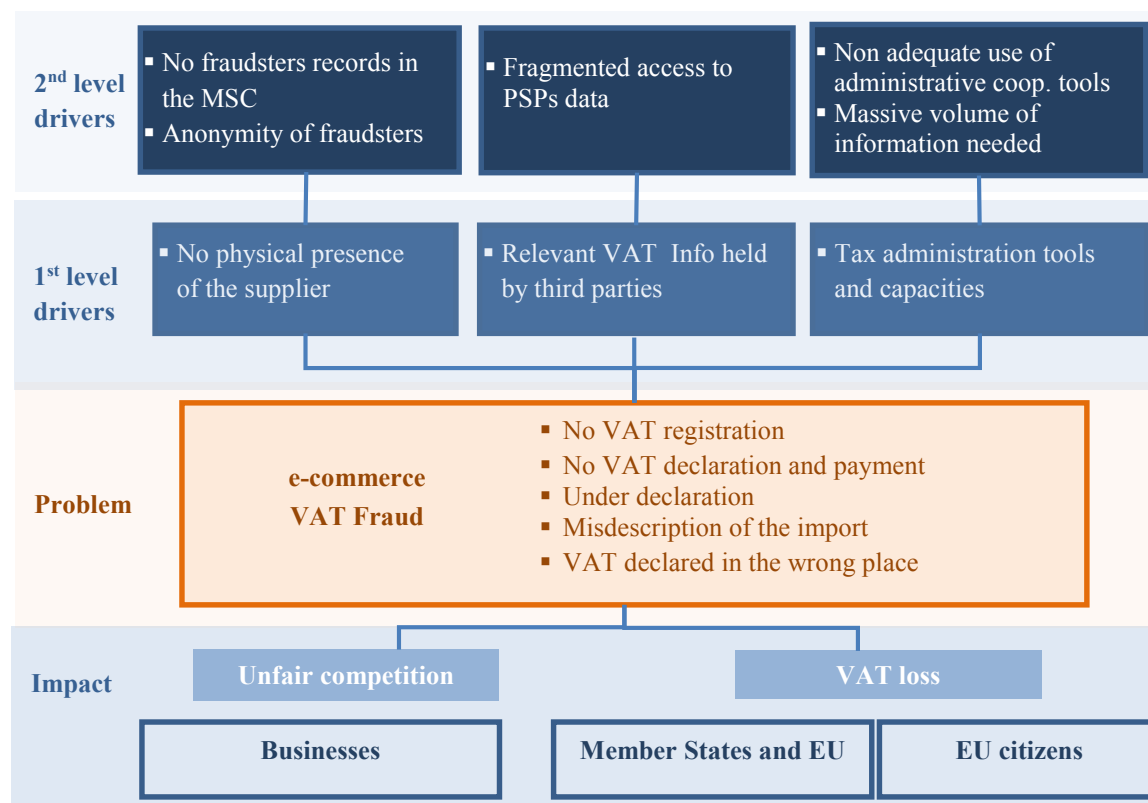
⁵⁴ Calculated as follows: £5 billion of sales excluding VAT would be needed to generate VAT, at 20%, of £1 billion; these two figures added together equal £6 billion gross sales revenue. £7.5 billion of sales excluding VAT would be needed to generate VAT, at 20%, of £1.5 billion; these two figures added together equal £9 billion gross sales revenue. National Audit Office Investigation into overseas sellers failing to charge VAT on online sales, p. 20

A similar estimation of £7.5 billion has been done by a UK retailers' association named RAVAS See: <http://www.vatfraud.org/blog/750000000-in-lost-revenue-to-uk-companies/>

⁵⁵ Assuming that the EUR 2.6 – 3.8 of VAT loss is calculated at a standard rate of 20%, the equivalent net sale would be EUR 13-19 billion

2.3. Problem tree

Figure 3: Problem tree



2.4. What are the problem drivers?

2.4.1. No physical presence of the suppliers

No fraudsters' records in the MSC

E-commerce allows online-performed key functions common to all business models such as bringing buyers and suppliers together (i.e. own online-shop, search engines, referrals, third party marketplace); providing a safe environment to conduct transactions for buyers and suppliers (i.e. own online-shop, trust facilitators, third party marketplace); processing payments from buyers to suppliers, including payment service providers (PSPs) and payment gateways (i.e. payment intermediators, on-platform payments, direct payments through bank transfer, direct debit, cash); delivering products (goods or services) from suppliers to buyers (i.e. delivery and fulfilment managed by marketplace, by third party logistic organization, by own means).

The supplier can insource or outsource all these functions, or use a combination of insourcing and outsourcing, but does not need a physical presence to get in contact with the clients or to deliver its products to its clients. Therefore, in the MSC the records needed to assess VAT liabilities might not be available or their quality/reliability may be very poor (e.g. in case of importation of goods, an invoice is not mandatorily accompanying the consignment).

Furthermore, in B2B transactions the reporting obligations for businesses claiming VAT in the MSC allow tax administrations to reconstruct the transaction chain. This is not the case for B2C sales, because the final consumer does not have similar record-keeping obligations. Information on B2C supplies are available to MSCs' tax authorities only if the supplier registers, declares and pays in those MSCs or through the MOSS portal. If this is not the case, the MSC will lack VAT records or immediate information to collect

data for the control of VAT liabilities. The lack of VAT identification numbers and records also affects tax authorities' possibility to carry out risk analysis, because they may even be unaware of suppliers selling online in their own Member State.

Due to this poor quality of information available in the MSC, tax administrations have limited means to (1) identify the sellers; (2) detect taxable supplies in their own jurisdiction; (3) understand whether the remote sellers are taxable persons that should pay VAT in the EU; and (4) assess VAT liabilities.

Anonymity of fraudsters

In e-commerce VAT fraud, where B2C cross-border transactions are at stake, the internet, as demonstrated above, allows the supplier to hide its own identity behind a domain name⁵⁶. Even when a tax authority is aware of the existence of a given online shop, the identity of the business behind it, its real location or its turnover in that Member State remain unknown. It is important to note that the objective of the tax authorities is to detect the fraudulent businesses hiding behind the online shops.

2.4.2. Relevant VAT information held by third parties

Intermediaries such as online marketplaces and PSPs are involved in the trade chain without being a party in the sales contract between suppliers and buyers. In 2014, e-retailers covered 30% of the total global market share. The three biggest firms (Amazon, eBay and Alibaba) provided 65% of the global e-retailer sales and 94% of payments for cross-border online purchases use electronic payment systems, credit or debit cards, or prepaid cards⁵⁷.

Fragmented access to third party data

In 2016, the Commission services launched a survey with the tax administrations of the Member States⁵⁸ on e-commerce VAT anti-fraud policies. The survey showed that only less than half of the respondent Member States collect data from digital platforms (or their branches) established in their own jurisdiction for VAT control purposes, while around half of them replied that they collect VAT relevant data from payment intermediaries⁵⁹. However, the type of PSPs involved in the transmission of data to tax authorities varies from Member State to Member State (e.g. credit card companies, banks and financial institutions, or others...). The format and the way data is collected also differs (some Member State collect payment data only on specific cases of tax audits, others all payment transactions on regular basis, etc...).

Moreover, even in the cases where structured forms of cooperation between tax authorities and third parties have been established, there are emerging criticalities. In fact, Member States do not always receive the information from payment intermediaries and sometimes they get it with either significant delays or referring to a limited period. Often third parties are not providing the information because they only have a branch in the requesting Member State while the information requested is under another jurisdiction. Finally, tax administrations' non-targeted requests to identify online sellers (bulk requests) are problematic to be dealt with and are often not replied by third parties.

Conversely, internet platforms can help tax administrations when they receive targeted requests on specific cases. For instance, eBay developed electronic systems that law

⁵⁶ A domain name is a unique name that gives an identity on the internet. The first part of the domain name is the name itself (e.g. 'thisisme2'). The second part of the domain name is the extension (the bit that comes after the final dot – e.g. .be, .brussels, .com, .eu and many more).

⁵⁷ International Post Corporation, e-Commerce logistic and delivery, eCom21 2016.

⁵⁸ See 10.8 - Annex 8: Result of the TAXUD 2016 survey on e-commerce compliance strategies in the EU

⁵⁹ See 10.2 - Annex 2: Consultation synopsis report, section 3.2

enforcement and tax authorities can use to make targeted requests referring to the eBay platform⁶⁰. However, as stressed in section 2.4.1. e-commerce VAT fraudsters are often unknown and the tax authorities have difficulties in addressing targeted requests.

2.4.3. Tax administration tools and capacities

Non adequate use of administrative cooperation tools

When a given supplier, or the third party (i.e. online market place or PSPs) holding the relevant information on that supplier, are established in another Member State, the authorities of the MSC must ask the tax authority of that Member State to receive some relevant information through the administrative cooperation instruments under Regulation (EU) No. 904/2010. Where the fraudsters and their location are unknown, identifying the Member States where to address a request for administrative cooperation is a problem *per se*.

Usually, the first need of a tax authority is to identify "potential" taxable persons performing economic activities giving rise to VAT liabilities in its own jurisdiction. This could result in bulk "identification requests" either to a third party (i.e. online market place or PSPs) holding this information or to a tax authority of a country where the third party is established.

However, Council Regulation (EU) No. 904/2010 lays down rules for cooperation between competent authorities of the Member States, and not between competent authorities and third parties. Furthermore, under that Regulation, a Member State cannot be requested to transmit "bulk data" to a requesting Member State. Such a request would be considered disproportionate under Article 54(1). Finally, under Article 54(2), Member States cannot be required to provide information if the national legislation does not authorise them to collect it. This limits the possibilities for Member States to request third party data from other Member States. In fact, half of the respondent Member States to the 2016 survey reported difficulties in receiving information from other Member States on e-commerce B2C fraud. Still, a competent authority aware of any potential breach to the VAT legislation in another Member State can send spontaneous information. However, according to the 2016 survey only five Member States reported to have received such spontaneous information from another tax administration under Regulation (EU) No. 904/2010.

Massive volume of information

VAT is a consumption tax levied as a percentage of every single transaction. This makes the tax administrations' task of controlling cross-border B2C supplies particularly challenging in view of the volume of online purchases. In 2014 cross-border e-commerce across the EU-28 was estimated at EUR 96.8 billion⁶¹ (which represents 18% of the total online spending in the EU-28). This corresponds to several billion cross-border purchases⁶² across Europe. Part of these cross-border transactions is declared to tax

⁶⁰ LERS – Law Enforcement which is portal that allow to law enforcement and tax authorities to submit targeted requests eRequest System, see: <https://lers.corp.ebay.com/AIP/portal/home.do>
LEP Law Enforcement Portal which is a tool that allows law enforcement and tax authorities to obtain targeted eBay user information without the need of submitting a data request, see: <https://lep.corp.ebay.com/leportal/lep/login.do>

⁶¹ The majority of this spending comes from within the EU, with non-EU spending accounting for 28% of cross-border e-Commerce. Over 70% of the EU28's cross-border spending originates from sellers in other EU Member States; about 30% originates from the rest of the world. Source: Deloitte 2015 "VAT Aspects of cross-border e-commerce - Options for modernisation" Final report – Lot 1, page 16

⁶² The Payments Statistics Report published by European Central Bank shows 7 billion cross-border payments in the EU in 2016. European Central Bank, Payments Statistics, see: <http://sdw.ecb.europa.eu/reports.do?node=1000004051>

authorities (i.e. through direct registration and declaration in the MSC or through the MOSS for TBE services⁶³). However, there are still instances of non-compliance or even fraud in ecommerce transactions for which the tax authorities need additional sources of information for their control activities in order to cross-check the VAT declarations, verify the correct assessment of VAT liabilities and detect instances of non-declaration or fraud. The huge volume of data at stake requires adequate administrative capacity in terms of IT and analytical resources. However, only a very small minority of Member States (6 positive answers out of 23 in the targeted consultation) indicated to have in place a kind of risk analysis system of third party data to detect e-commerce VAT fraud⁶⁴.

2.4.4. Other Drivers influencing e-commerce VAT fraud (and addressed by other initiatives)

The way goods are controlled at the moment they are introduced into the internal market has an impact on VAT fraud. In particular, because of the huge amount of parcels entering the internal market, the importations of parcels of low value (benefiting from the VAT exemption for small consignments) and of the ones not exceeding the threshold of EUR 150 (benefiting from the exemption from customs duties) results in significant lack of control by customs and VAT authorities⁶⁵. This issue has been addressed by another legislative initiative described under section 5.1 of this report.

2.5. How will the problem evolve?

In 2016, the e-commerce turnover increased by 15% in Europe and it was expected to reach over EUR 600 billion in 2017⁶⁶, suggesting that the penetration rate of e-commerce will continue to climb. This could potentially generate an increasing impact of VAT fraud in the coming years. On the one hand, consumers are becoming more and more confident with buying online and businesses can benefit from a growing e-commerce market. On the other hand, fraudsters benefit from the same opportunities if tax administrations are not provided with the appropriate instruments to fight e-commerce VAT fraud.

3. WHY SHOULD THE EU ACT?

As demonstrated under section 2, the origin of the problem is wide-ranging: the economic trend of consumers buying online from various jurisdiction, the VAT rules that correctly seek taxation in the Member State of consumption, the huge and unstructured amount of information available in an e-commerce framework, the fact that such information is not directly available to tax administrations and the limitations of the administrative cooperation framework.

⁶³ The number of transactions declared under the MOSS is not available. However, the number of businesses registered to the MOSS as provided by Member States in the Union scheme totalled 12.899. The number of registrants in the Non-Union scheme totalled 1 079. About 34.000 businesses supplying TBE services are compliant outside the MOSS through direct registration while 36.000 are estimated to be outside the system. Source Deloitte study on VAT Aspects of cross-border e-commerce - Options for modernisation, Lot 3, p. 15

⁶⁴ See 10.2 - Annex 2: Consultation synopsis report, section 3.2.

⁶⁵ SWD(2016)379 final of 1.12.2016 Impact Assessment accompanying the document "Proposal for a Council Directive, a Council Implementing Regulation and a Council Regulation on Modernising VAT for cross-border B2C e-Commerce", p. 16.

Copenhagen economics "e-commerce imports into Europe: VAT and Customs treatment

See: <https://www.copenhageneconomics.com/publications/publication/e-commerce-imports-into-europe-vat-and-customs-treatment>

⁶⁶ Ecommerce Europe European Ecommerce Report 2017

The public consultation confirmed that the problem of VAT fraud in e-commerce concerns all the EU Member States. The majority of the respondents (34 out of 52) considered that the problem should be addressed at both EU and Member States level while many (14) were of the opinion that e-commerce VAT fraud should be addressed at EU level only. In the targeted consultation, 17 tax authorities out of 23 confirmed that Member States alone are not able to fight VAT fraud in e-commerce without using the administrative cooperation.

The European Court of Auditors noted that e-commerce poses challenges to Member States in terms of VAT collection especially because of a lack of information on B2C cross-border supplies⁶⁷.

The VAT Forum subgroup on e-commerce⁶⁸ recognised that whereas business understands the data needs of tax authorities it should be made as easy as possible for business to provide the relevant data (consistent data sets).

The administrative cooperation framework is laid down in Council Regulation (EU) No. 904/2010. The way Member State tax administrations cooperate to fight VAT fraud has an impact on the internal market. Individual Member States cannot achieve the objective of ensuring a sound anti-fraud system to protect the internal market from VAT fraud unless they coordinate at EU level. It should be noted that Regulation (EU) 904/2010 also provide for a clear legal base indicating the sources of the information to be exchange by Member States' tax authorities through the electronic systems (e.g. VAT national databases, MOSS information...) ⁶⁹. Therefore, any new form of exchange of data should be regulated under the same Regulation. The VAT Directive lays down the record keeping obligations of taxable persons and intermediaries⁷⁰ and, thus, any new record keeping obligation for payment service providers should be foreseen under the VAT Directive. Furthermore, implementing legislation will have to be adopted in order to implement any new tool for administrative cooperation and to detail any new VAT obligation. Also the 75% of European citizens think that the EU should intervene more than at present in the fight against tax fraud, as indicated in the June 2016 Eurobarometer⁷¹.

The legal basis is Article 113 of the Treaty on the Functioning of the European Union.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objectives

The general objectives of the initiative are

- to reduce the VAT loss for the Member States, thus contributing to the fiscal consolidation within the EU;
- to level the playing field for the legitimate businesses in the EU that suffer from unfair competition by fraudsters.

⁶⁷ Tackling intra-Community VAT fraud: More action needed (Special Report from European Court of Auditors, No 24 of 2015), See:

https://www.eca.europa.eu/Lists/ECADocuments/SR15_24/SR_VAT_FRAUD_EN.pdf

⁶⁸ https://ec.europa.eu/taxation_customs/sites/taxation/files/d-1507602_report_consolidated_en.pdf

⁶⁹ Article 17 of Council Regulation (EU) 904/2010 indicates

⁷⁰ Council Directive 2006/112/EC Chapter XI

⁷¹ See: http://www.europarl.europa.eu/external/html/eurobarometer-062016/default_en.htm#taxfraud

4.2. Specific objectives

The specific objective is to reduce e-commerce VAT fraud by providing tax authorities with efficient and effective instruments for detecting non-compliant businesses.

At this regard it should be noted that, as described in section 2, the problem at stake refers to businesses with a real economic activity online, but defrauding VAT by not registering for VAT purposes, not declaring and paying the due VAT. As such the fight against these fraudsters is the specific objective of the initiative.

4.3. Operational objectives

The operational objectives are:

- To give EU Member States' tax administrations access to relevant third party data to fight e-commerce VAT fraud
- To improve the identification and targeting of potential e-commerce VAT fraud
- To offer new or improved channels for EU Member States' tax authorities to access and share third party VAT-related information

4.4. Consistency with other EU policies and with the Charter for fundamental rights

The objective of fighting tax fraud and evasion to help secure national and EU revenues and prevent distortion of competition is amongst Commission priorities. The political guidelines⁷² of the present Commission called for stepping up the efforts to combat tax evasion and tax fraud, including through improved administrative cooperation between tax authorities.

The proposal under consideration will trigger new exchanges and processing of VAT-related information and personal data. The General Data Protection Regulation (GDPR)⁷³ gives a wide definition of personal data including any information relating to an identified or identifiable natural person that can be identified directly or indirectly. As such the payment data listed above contains information falling under the scope of the GDPR and the principles for the protection of personal as laid down in the Charter of Fundamental Rights⁷⁴. The GDPR fixes the principles and data subjects rights to be respected while processing personal data. However, the Union may restrict by legislative measures these principles and the rights of the data subject – as long as the restrictions respect the principles of necessity and proportionality – to safeguard important objectives of general public interest of the Union, such as economic and financial interest including taxation⁷⁵. The impact of the different options on protection of personal data will be detailed under section 6 after the detailed description of the different options⁷⁶.

⁷² See: https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en_0.pdf

⁷³ Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1

⁷⁴ Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391

⁷⁵ Article 23 GDPR

⁷⁶The assessment of the principles of necessity and proportionality has been done in line with the European Data Protection Supervisor (EDPS) toolkit, which also takes into account the relevant jurisprudence of the Court of Justice of the European Union (hereafter CJEU), the European Court of Human Rights (ECtHR), and previous Opinions of the EDPS See: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf. For the jurisprudence see: See: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

As indicated in section 2.1 the VAT loss on e-commerce is also due to the complexity of the VAT system. This was addressed by recent Commission's measures, shortly described here below in section 5.1.

5.1. Measures with a positive impact on reducing the e-commerce VAT loss introduced with the VAT e-commerce package)

5.1.1. Abolition of the distance sale thresholds and extension of the MOSS

The current distance sale thresholds represent a complication for the European businesses that must be aware of the different rules in the different Member States they are supplying to, and in the case where the threshold is exceeded they must deal with different tax authorities and procedures⁷⁷. As from 1 January 2021, the distance sale threshold will be replaced by a new EUR 10.000 intra-EU cross-border threshold. The EUR 10.000 threshold will refer to the total value, exclusive of VAT, of the supplies of goods and TBE services to consumers in any Member State other than the Member State of the supplier in the course of the preceding calendar year⁷⁸. When the total annual intra-EU cross-border turnover of a given supplier does not exceed the threshold the place of supply remains in the Member State of the supplier. When the threshold is exceeded, the destination principle will apply (and the supplier will have to register in the Member States of consumption or in in the MOSS)⁷⁹. The abolition of the thresholds together with the extension of the MOSS to all cross-border supplies of goods and services will make the VAT system easier to comply with. Still tax authorities need relevant information to control the new EUR 10.000 thresholds, and detect non-registered distance sellers and their real turnover in the MSC.

5.1.2. Abolition of the small consignments exemption

As described in section 2.1.3 the small consignments exemption is abused to avoid the payment of VAT on importations. As from 1 January 2021 the exemption on small consignments will be abolished⁸⁰. Still tax authorities will need tools to control the real value of goods imported in case of under-declarations.

5.1.3. Import One Stop Shop (IOSS)

Also imports of parcels of a value over the small consignments exemption but under the EUR 150 customs threshold⁸¹ raise concerns as regard the way VAT is declared and paid.

⁷⁷ SWD(2016)379 final of 1.12.2016 Impact Assessment accompanying the document "Proposal for a Council Directive, a Council Implementing Regulation and a Council Regulation on Modernising VAT for cross-border B2C e-Commerce", p. 14

⁷⁸ Article 59c of VAT Directive as amended by Council Directive (EU) 2017/2455 of 5 December 2017 amending Directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations for supplies of services and distance sales of goods, OJ L 348, 29.12.2017, p. 7

⁷⁹ Under the EUR 10.000 threshold the micro-businesses will benefit from a VAT exemption on their domestic transactions (as long as permitted by the national legislation), and they will not have to register in other Member States or in the MOSS starting from the first intra-EU sale

⁸⁰ Article 3 Council directive (EU) 2017/2455 of December 2017 amending Directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations for supplies of services and distance sales of goods

⁸¹ Customs Duty is not due for goods, provided directly to the buyer when their value does not exceed 150 euros. See https://ec.europa.eu/taxation_customs/individuals/buying-goods-services-online-personal-use/buying-goods/buying-goods-online-coming-from-a-noneu-union-country_en

It was estimated that there were 43 million such imports in 2015. A study⁸² found that VAT is not paid on 65% of consignments from non-EU suppliers through the public postal channels⁸³. This is significant as it is estimated that 70% of transactions are sent through public postal channels. As from 1 January 2021, an Import One Stop Shop (IOSS) regime will be set up⁸⁴. The IOSS will streamline the VAT registration, declaration and payment process. Tax authorities will still have the need to detect the suppliers remaining outside the VAT system and to crosscheck the correctness of the information received through the VAT declarations from the taxpayers registered in the VAT system.

5.1.4. Deemed supplier

As described in section 1.1, under the deemed supplier provision⁸⁵ from 2021 online market places, platforms and portals will have to fulfil the VAT declaration and payment obligations for certain goods⁸⁶ sold through their intermediation by non-EU taxable persons. Also the “deemed supplier” provision has been introduced to streamline the VAT declaration and payment process. The tax authorities will still need tools to control the correctness of the VAT declarations and payments.

5.2. Policy options

The options have been designed after consultation with Member States and businesses representatives in the framework of the VAT forum subgroup on e-commerce⁸⁷. It should be noted that, as described in section 1 this initiative has to be seen as complementing the wider VAT e-commerce compliance framework where the new legislation created new VAT responsibilities for electronic interfaces such as internet marketplaces and platforms (under the deemed supplier provision). In addition to the baseline, the proposed options seek the solution to the problem described in section 2 in a better cooperation between tax authorities and PSPs. In fact, the payment is the consideration of any purchase of goods and services. In the last years more than 90% of online purchases by European customers went through credit transfers⁸⁸, direct debits⁸⁹ and card payments⁹⁰, thus

⁸² E-Commerce Imports Into Europe: Vat And Customs Treatment (2016) See: <https://www.copenhageneconomics.com/publications/publication/e-commerce-imports-into-europe-vat-and-customs-treatment>

⁸³ In the vast majority of cases, the customer is not charged VAT at the time of sale but rather the package is assessed for VAT at importation in the territory of the European Union. The customer pays the VAT and an administrative fee is charged to the customer by the transport operator i.e. the express courier or postal operator at the point of delivery of the good to cover the administrative costs of clearing customs.

⁸⁴ Under the new import One-Stop Shop (IOSS) – introduced by Council Directive (EU) 2017/2455 of 5 December 2017 unlike today VAT can be collected at the point of sale to EU customers by sellers or market places. Non-EU sellers will then declare the VAT using the IOSS. These goods will then benefit from a fast-track customs mechanism.

⁸⁵ New Article 14a of the VAT Directive as amended by Council Directive (EU) 2017/2455 of 5 December 2017 amending Directive 2006/112/EC and Directive 2009/132/EC as regards certain value added tax obligations for supplies of services and distance sales of goods, OJ L 348, 29.12.2017, p. 7

⁸⁶ In particular for a) distance sales of goods imported from third territories or third countries not exceeding the value of EUR 150 and b) the B2C supplies of goods which are already in the EU (i.e. in fulfilment centers) by non-EU established taxable persons facilitated through these platforms.

⁸⁷ Commission Decision 2012/C 198/05 of 3 July 2012 setting up the EU VAT Forum, OJ C198 of 6 July 2012; See: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012D0706%2802%29>

⁸⁸ A credit transfer is a payment initiated by the payer. The payer sends a payment instruction to his/her payment service provider (PSP), e.g. a bank. The payer’s PSP moves the funds to the payee’s PSP. This can be carried out via several intermediaries.

⁸⁹ A direct debit is a transfer initiated by the payee via his/her payment service provider. Direct debits are often used for recurring payments, such as utility bills. They require a pre-authorisation (or “mandate”)

through an intermediary involved in the transaction⁹¹ and this is a trend that will continue in the future⁹².

As such third parties holding payment data can give a complete picture to tax authorities to properly carry out their basic task of controlling the correct fulfilment of VAT obligations on cross-border B2C supplies of goods and services. The experience of the Member States that already cooperate with PSPs at national level showed how cooperation with PSPs gives tangible results in fighting e-commerce VAT fraud⁹³. Furthermore, also some non-EU countries are using payment service data as a tool for detecting non-compliant traders in combination with simplified collection regimes for cross-border B2C supplies of goods (similar to the EU system)⁹⁴.

It should be noted that – unlike in the VAT area – in other fields of taxation there is already a European legislative framework regulating the cooperation between third parties and tax authorities. The so-called Savings Directive⁹⁵ foresees that "payment agents" must report to the competent authority of the Member State where they are established a minimum amount of data as regard the beneficiary of the interest payments. Furthermore, in the field of direct taxation⁹⁶ each Member State shall take the necessary measures to require its Reporting Financial Institutions to transmit data on personal income and financial account information. In both cases, after the acquisition of the information, tax administrations exchange the relevant data between them.

Furthermore, money flow information is also considered important to fight against illicit activities in other fields. Under the current Anti-Money Laundering Directive⁹⁷ obliged entities must retain a series of documents and information for the purpose of preventing, detecting and investigating possible money laundering and terrorist financing and are required to report suspicious transactions and activities to Financial Investigations Units. Following the Action Plan against terrorist financing (2016), the Commission is analysing possible new EU systems to track the money flow⁹⁸.

from the payer. Direct debits are also used for one-off payments. In this case, the payer authorises an individual payment.

⁹⁰ Debit cards allow the cardholder to charge purchases directly to his/her bank account. Credit cards provide the cardholder with a certain credit limit, within which he/she can make purchases. The credit card holder must pay off the balance in full by the end of a specified period. Alternatively, he/she can pay off part of the balance. The remaining balance is taken as extended credit on which the cardholder must pay interest.

⁹¹ E-shopper barometer 2017(DPDgroup). See: https://www.dpd.com/be_en/business_customers/dpd_insights/e_shopper_barometer_2017 and International Post Corporation, e-Commerce logistic and delivery, eCom21 2016

⁹²

See: <https://www.atkearney.com/documents/10192/1448080/Winning+the+Growth+Challenge+in+Payments.pdf/b9da93a5-9687-419e-b166-0b25daf585ff> p. 5

⁹³ In particular the Finnish tax administrations was able to collect EUR16 million in 2016 based on cooperation with payment service providers

⁹⁴ See Annex 11 "Third countries using payment data as VAT control tool"

⁹⁵ Council Directive (EU) 2015/2060 of 10 November 2015 repealing Directive 2003/48/EC on taxation of savings income in the form of interest payments OJ L 301, 18.11.2015, p. 1

⁹⁶ Council Directive 2014/107/EU of 9 December 2014 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation In force OJ L 359, 16.12.2014, p. 1

⁹⁷ Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) In force OJ L 141, 5.6.2015, p. 73

⁹⁸ See: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/tftp_en

Payment data is also considered as a possible source of intelligence in Customs controls for risk management purposes by the World Customs Organisation (WCO) under the 2018 "cross-border e-commerce framework of standards"⁹⁹.

It is clear that these different policy objectives are regulated by different European legal acts: illicit activities in different fields have different patterns that require different kind of data or different methodologies for the data collection, analysis and exchange. However, the legislative framework shortly described above shows a clear trend toward cooperation between different public authorities and payment and financial institutions with the aim of enhancing the fight against illicit activities.

5.2.1. Payment services and payment service providers¹⁰⁰

The payment data in the regulatory option will refer to data on credit transfers, direct debits and cards payments because – as mentioned above – they represent almost the totality of the purchases online. Therefore, the providers of that kind of payment services will be in the scope of the regulatory option.

Virtual currencies (VCs), better known as crypto-currencies, are not within the present initiative. There are two reasons for that. First, cryptocurrencies are at present very rarely used for the type of transaction covered by this initiative and this does not seem likely to change in the near future. Secondly, they are not regulated in the European legal framework and in particular in the SEPA regulation and the Payment Service Directive 2. It should be noted that, as also stressed in the 2016 European Banking Authority's (EBA) opinion on virtual currencies¹⁰¹, VCs incur technology specific risks that makes them distinct from conventional fiat currencies and do not make them – so far – a safe payment method.

As such VCs are not part of this initiative. There is a potential, but not short-term, risk that part of e-commerce VAT fraud could migrate to this kind of payment. The risk appears limited at present because the volatility of cryptocurrencies exposes traders to a higher exchange rate risk than the potential gains from VAT non-payment. However, the regulatory option will foresee a periodic report of the Council which could eventually bring to a review of the scope.

5.2.2. Payment data

Only the data referring to cross-border payments¹⁰² that will allow tax authorities to detect the e-commerce VAT fraud patterns listed under point 2.1 of this report will fall within the scope of this initiative. In particular, payment data will refer to the:

- Identification of the supplier (payee)¹⁰³: name, address, any kind of tax number ...
- Total amount of the payment transaction
- Date of the payment transaction
- Country of origin of the payment

⁹⁹ Resolution Of The Policy Commission Of The World Customs Organization On The Guiding Principles For Cross-Border E-Commerce (Luxor, December 2017).

¹⁰⁰ See Annex 9, Payment services framework in the EU

¹⁰¹ EBA-Op-2016-07, 11 August 2016

¹⁰² To have an idea of the volume of data, the Payments Statistics Report published by European Central Bank shows 7 billion **cross-border payments** in the EU in 2016. European Central Bank, Payments Statistics, see: <http://sdw.ecb.europa.eu/reports.do?node=1000004051>

¹⁰³ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) OJ L 337, 23.12.2015, p. 35, Article 4(8).

- Description of the supply underlining the payment transaction (good or service) – if available to the payment service provider
- Unique identifier¹⁰⁴ for a payment transaction.

The data to be exchanged are the same under all options. This is because each of the elements listed above is indispensable to make the records useable by tax authorities for VAT anti-fraud purposes.

5.2.3. Structure of the policy options

This impact assessment takes into account **three alternative policy options**:

1. In the baseline (status quo) scenario the tax authorities of the EU Member States follow different approaches to fight against e-commerce VAT fraud and only some of them collect data from online intermediaries;
2. Under the non-regulatory option the European Commission helps tax authorities to develop their administrative capacity to fight e-commerce VAT fraud and publishes guidelines in order to enhance the cooperation between tax authorities and payment intermediaries;
3. The regulatory option implies the amending of the EU legal framework:
 - ✓ for the PSPs to keep records of VAT relevant payment data that will have to be transmitted to the tax authorities (transmission of payment data from PSPs to tax authorities);
 - ✓ for the tax authorities to collect payment data and exchange or share these data with other Member States' tax authorities (exchange of data);
 - ✓ for the tax authorities carry out a risk analysis to detect remote suppliers not complying with VAT obligations (risk analysis);

In particular, the regulatory option will imply amending the VAT Directive as regards the new record-keeping obligations of the PSPs, and Council Regulation (EU) 904/2010 as regards the exchange of payment data between tax authorities.

Under the regulatory option, different alternative technical solutions are envisaged to make tax authorities exchange or share the relevant payment data.

The regulatory option does not foresee a direct access of Member States' tax authorities to PSPs' databases because it would not be proportionate to the objective of fighting e-commerce VAT fraud. In fact, a direct access to PSPs' databases would disclose to tax authorities data which are not strictly necessary for the purpose at stake, i.e. information on the payers and on domestic payments. In fact it is important to note that the objective of the initiative is to target fraudulent businesses selling online, and not the consumers buying online. As such, payers data (i.e. data regarding the consumers paying for the purchases of products online) are not included in the scope of this initiative that does not aim at revealing the costumers behind an account.

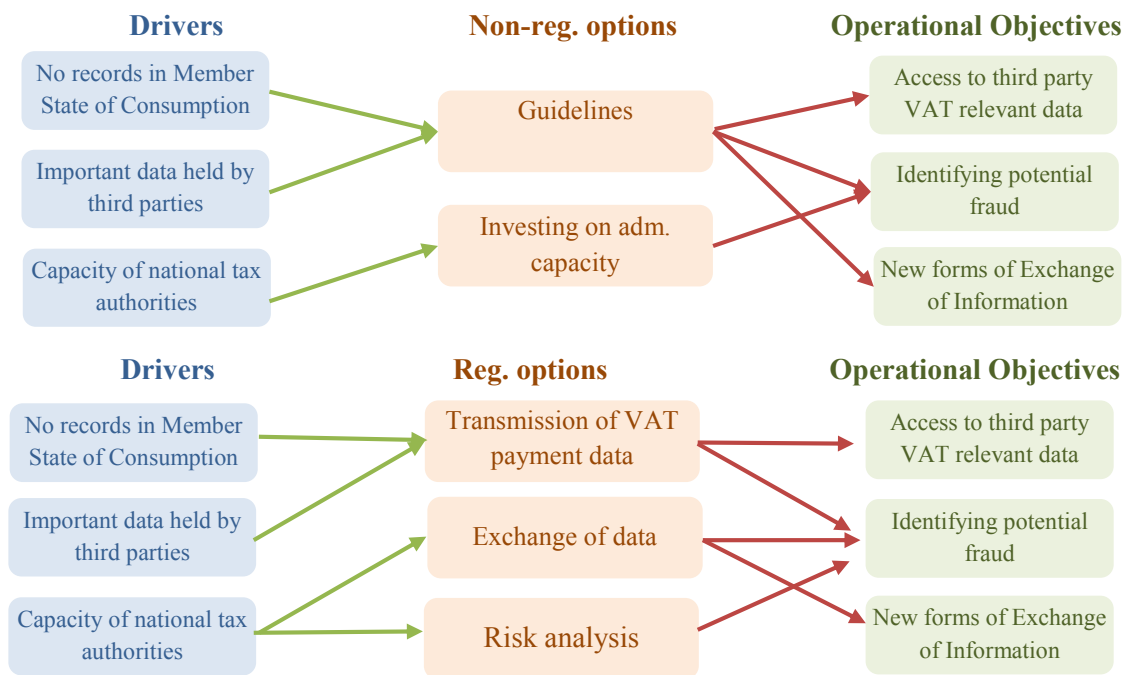
Finally, payment data are needed to detect the fraudsters. However, currently not all Member States have access to this kind of data. Few Member States collect payment data systematically (i.e. every month or every quarter) while other only on specific cases, in order to support the finding of an open VAT control. The initiative will make cross-border payment data available to all Member States in the same way, with the same set of information and with the same periodicity (quarter reporting obligations of PSPs). Only the PSPs established in the Member States will be subject to the reporting obligations foreseen in the regulatory options. It should be noted that, in a payment transaction there usually are at least two payment intermediaries: one acting on behalf of the payer and one acting on behalf of the payee. Both must have the information on the payer and payee in order to execute the payment transaction. As described in section 2 the European

¹⁰⁴ Directive (EU) 2015/2366, Article 4(33).

consumers are not directly involved in the fraud. Therefore, even when they buy from suppliers established in third countries, they keep using their own preferred and trusted payment methods and intermediary. Therefore, the payment service providers acting on behalf of the European payers will provide tax authorities with the necessary information to detect the recipient of the funds even when established outside the EU, and this without disclosing the information on the customer.

The regulatory options do not foresee any additional obligation to the taxable persons supplying goods and services (both online and in the "traditional" market).

Figure 4: Link between drivers, options (non-regulatory and regulatory) and specific objective



5.3. What is the baseline from which options are assessed?

5.3.1. Policy option 1 – Baseline scenario

As mentioned in section 2.4.2, the survey launched with tax authorities in 2016¹⁰⁵ showed that only one third of the Member States¹⁰⁶ collect data relevant for VAT controls from online market places, platforms and portals established in their own jurisdiction. The targeted consultation showed that twelve of the respondent Member States¹⁰⁷ collect data from PSPs established in their own jurisdiction. Member States have no statutory right to request payment data from taxpayers established abroad. Third party data are also used in combination with other tools i.e. cooperation with the national Financial Investigation Unit/Anti-Fraud Unit (15 Member States), national custom authorities (15 Member States), post offices (10 Member States), transport and logistic companies (8 Member States), online market places (9 Member States), use of internet monitoring tools (15 Member States).

¹⁰⁵ See Annex 8 "Result of the TAXUD 2016 survey on e-commerce compliance strategies in the EU"

¹⁰⁶ Only seven Member States out of the 21 Member States that replied to the survey communicated to have a sort of cooperation with online market places, platforms and portals.

¹⁰⁷ See Annex 2 "Consultation synopsis report", section 3.2

However, the Member States could not indicate whether this information was useful to fight e-commerce VAT fraud. It should be noted that, as mentioned in section 5.2. of this report, different policy objectives are regulated by different legal basis, and also the information transmitted by financial institutions to different national authorities is different depending on the purpose.

As regard international cooperation under the framework of Regulation (EU) 904/2010, the Member States set up a new Working Field dealing with e-commerce in Eurofisc¹⁰⁸. However, also in Eurofisc the legal constraints mentioned in section 2.4.3 apply. Member States make very little use of request for information and rarely send spontaneous information in the field of e-commerce (see section 1.2). Finally, the recently adopted amendments to Regulation (EU) 904/2010 (see section 1.2) do not address e-commerce. The envisaged cooperation between Eurofisc and Europol and OLAF will refer to specific information on VAT fraud cases related with criminal organisations.

Furthermore, three Member States¹⁰⁹ indicated that the tax administration has the legal authority to **take down the domain name**¹¹⁰ of web-shops because of breaches to the VAT legislation, independently or in collaboration with another agency (i.e. consumer protection agency).

Finally, the VAT Directive¹¹¹ allows Member States to provide that a person other than the person liable for the payment of VAT is to be held jointly and severally liable for payment of VAT. Even though three Member States indicated to have general national regulation that entails VAT responsibility for internet platforms under certain circumstances, the 2016 survey showed that this opportunity is used to a limited extent.

Different from the Joint and Several liability is the "deemed supplier" provision introduced by the new Article 14a of the VAT Directive that will enter into force as from 2021 (as described in Section 1.1 of this Report). Under the Joint and Several Liability a third party is held responsible for the payment of VAT under certain conditions, i.e. if it is involved in a fraud and the third party 'knew or should have known' about the fraud. On the contrary, under the "deemed supplier" provision the third party is directly considered as a liable person because it is "deemed" to have received and supplied the goods himself.

5.4. Description of the policy options

5.4.1. Policy option 2 (non-regulatory): Investing in administrative capacity and providing EU guideline + standard forms

This non-regulatory option would consist in strengthening cooperation among EU tax authorities in the following ways:

- *Investing in administrative capacity*

¹⁰⁸ Eurofisc is a network for the multilateral exchange of targeted information to combat VAT fraud. The legal basis is in Chapter X of Council Regulation (EU) No 904/2010.

¹⁰⁹ See Annex 8: Result of the 2016 TAXUD survey on e-commerce compliance strategies in the EU

¹¹⁰ A domain name is a unique name that you register for yourself, your company or organisation. Your domain name gives you an identity on the internet and provides other people with an easy way of locating you. A domain name is made up of a minimum of two parts, separated by a full-stop or dot. The first part of the domain name is the name itself (e.g. 'thisisme2'). The second part of the domain name is the extension (the bit that comes after the final dot). There are all sorts of extensions available: .be, .vlaanderen, .brussels, .com, .eu and many more.

¹¹¹ Council Directive 2006/112/EC Art. 205

The Commission can help the Member States to invest in administrative capacity to address e-commerce VAT fraud through the Fiscalis Programme¹¹² and Structural Reform Support Programme SRSP¹¹³. This is already the case in the framework of Eurofisc where the Fiscalis Programme is used to finance Working Field 5 (WF5) on e-commerce¹¹⁴.

- *Providing EU-level guidelines and (optional) forms for the Exchange of Information (EoI)*

The Commission, acting together with Member States and PSPs, could draft and publish guidelines to collect data from PSPs. Tax administrations could use these guidelines to ask the same set of data with a standard form. Such guidelines would however be optional and non-binding for both tax authorities and businesses. An example already exists in the field of the so-called Missing Traders fraud, where guidelines for cooperation between tax administrations and businesses to fight the Missing Trader fraud were drafted in 2016 by the VAT forum¹¹⁵ and published in TAXUD website¹¹⁶. Furthermore, the Commission, together with Member States could draft guidelines on how to use VAT relevant data from PSPs in order to detect fraudsters.

5.4.2. Policy option 3 (Regulatory option): Collection and exchange of payment data

Unlike the previous option, this option would introduce binding provisions directed at both PSPs and national tax authorities. This could be realised in different variants (sub-options).

Both sub-options work on the base of a “push” approach. The payment service providers will transmit every quarter the information to the tax authorities under both cases. The difference between the two sub-options is in the way Member States tax authorities will have access to the data and the data available to tax authorities.

To make the regulatory option more proportional a threshold is foreseen. In order to capture only the payments that are potentially linked to an economic activity (thus excluding cross-border payments executed for private reasons) a threshold linked to the number of cross-border payments received by a payee is foreseen: only when the total amount of payments received by a given payee exceeds the threshold of 25 payments in a 3 months period, the payment service providers will have to keep the records available to tax authorities on that payee. The threshold has been established taking into account an average value of online shopping orders of EUR 95¹¹⁷. An annual hundred payment transactions of that value will result in almost a total of EUR 10 000 which can already give raise to VAT obligations in the Member States, and matches with the EUR 10 000 threshold on intra-EU supplies introduced by the VAT e-commerce Directive.

5.4.2.1. Sub-option 3.1: Distributed application

*Phase I: Transmission of payment data to tax authorities*¹¹⁸

¹¹² See: https://ec.europa.eu/taxation_customs/fiscalis-programme_en

¹¹³ See: https://ec.europa.eu/info/funding-tenders/funding-opportunities/funding-programmes/overview-funding-programmes/structural-reform-support-programme-srsp_en

¹¹⁴ Eurofisc is a network where the competent officials of the Member States exchange data based on national risk analysis. Eurofisc Working Field 5 established in 2017 deals with the e-commerce control

¹¹⁵ For more information on the VAT forum, see: https://ec.europa.eu/taxation_customs/business/vat/eu-vat-forum_en

¹¹⁶ See:

https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/tax_cooperation/vat_gap/2016-03_guide-on-adm-cooperation_en.pdf

¹¹⁷ <https://www.statista.com/statistics/239247/global-online-shopping-order-values-by-device>

¹¹⁸ See Annex 12 "Visual examples of the regulatory options".

The PSPs will have to keep records of the data indicated in section 5.2.2. The retention period of these records for the PSPs will be two years, which is a proportionate balance between the necessary period for tax authorities to carry out controls and the obligation for PSPs to keep personal data. Then, every quarter¹¹⁹ the PSPs will transmit that set of VAT relevant data to the tax authority of the Member State where they are established using a single EU format (to be defined with implementing measures). The VAT relevant payment data will refer to all inbound and outbound payments (where either the payee or the payer are located in the EU) in the previous reporting period (and exceeding the 25 payments per payee in a calendar quarter)¹²⁰.

The VAT relevant payment data will be stored electronically by the tax authorities. The retention period will be defined by the national legislations but no longer than ten years, in lines with the general retention period obligation imposed to tax administrations under Regulation (EU) 904/2010¹²¹.

Phase II: Administrative cooperation between Member States - Exchange of data¹²²

As mentioned above, the VAT relevant payment data will be stored electronically at national level. The national databases will be connected through an electronic interface and distributed system available to all the tax administrations (similar to the VIES¹²³). Only the Eurofisc officials of the other Member States will have access electronically to the inbound and outbound payments from and to their own Member State. The Eurofisc officials of one Member State will have to access relevant data available in another Member State database logging a "search" in the system of the other Member State through the electronic interface. This will work in a similar way like the "automated access" currently regulated under Article 21 of Regulation (EU) 904/2010: the official starting the search should already have some piece of information in order to launch the research (i.e. an identification of a given taxpayer)¹²⁴. Then the system will show the result almost in real time. The result would be the payment transactions referring to a given payee, in a given period. Eurofisc is a network composed of anti-fraud officials of

¹¹⁹ Different reporting frequencies (daily, monthly, yearly) had been considered and discarded after consultation with Member States and payment service providers. The majority of the Member States indicated monthly, the PSPs quarterly. A monthly frequency implies administrative burdens to PSPs while quarterly still allow Member States to carry out appropriate controls

¹²⁰ A threshold of EUR 10.000 had been considered and discarded after the result of the targeted consultation. Under the threshold, the PSPs would transmit the payment data only when all payments received by a given payee exceed EUR 10.000. The threshold would be computed based on the payment received by a given payee during the previous reporting period.

The purpose of the threshold would be to exclude from the exchange of information the payments of small amounts that unlikely refer to a commercial activity. However, the this threshold as such would not be as such decisive to define an economic activity and could be easily abused by fraudsters by using multiple accounts to receive the payments. A threshold linked to the number of transactions has been considered more effective.

¹²¹ Article 55(5)(b) of Regulation (EU) 904/2010 as amended by COM(2017)706 final adopted by the Council on 22 June 2018

¹²² See Annex 12 "Visual examples of the regulatory options".

¹²³ The VAT Information Exchange System foresee in Chapter V of Regulation (EU) 904/2010 and that connect the national electronic systems of the Member States. The VIES makes available the information collected on intra-EU supplies (B2B only) on the basis of VAT registrations and the recapitulative statements submitted by taxpayers.

¹²⁴ Automated access is different than automatic exchange of information. The automated access gives the tax officials the possibility to search certain information in a database (Article 17 of Council Regulation 904/2010). Automatic exchange of information is the periodic exchange (on regular base e.g. monthly or quarterly or yearly) of a predefined set of data between tax authorities (Article 13 and 14 of Council Regulation (EU) 904/2010).

the Member States' tax administrations¹²⁵ for the multilateral exchange of information resulting from national risk analysis. Therefore, limiting the access to the system only to the Eurofisc officials will guarantee that the data can be used only for the detection of VAT fraud. Officials of the European Commission would have access to the system only for maintenance and development purposes.

Phase III: Risk analysis for control purposes

The inbound payments will allow the detection of domestic sellers while the outbound payments will allow the detection of remote sellers (established abroad). The system will not aggregate all payment data of a given payee in all the Member States. Therefore, if in one Member State there is relevant payment information referring to potential taxable transactions in another Member States, these Member States will not be alerted automatically by the system. In few words the risk analysis can only be carried out nationally by the tax authorities following their own national procedures. Based on the payment information retrieved from the system, the national Eurofisc officials will have to activate their own national tax administration to crosscheck this information with other sources of information, such as VAT, MOSS, customs' declaration and eventually carry out VAT controls.

5.4.2.2. Sub-option 3.2: Central storage¹²⁶

Phase I: Transmission of payment data to tax authorities

As for the sub-option 3.1. also under this sub-option the PSPs will have to keep records of the data indicated in section 5.2.2., and the retention period of these records for the PSPs will be two years. Then the transmission of the data from the PSPs to the tax authorities will be like in sub-option 3.1. Like in the previous sub-option, the tax authorities will store the payment data received in their own databases.

Phase II and III: Exchange of data and risk analysis for control purposes

The difference compared to sub-option 3.2 is in the way the tax authorities share amongst them the payment data and on the risk analysis. Under this sub-option the tax authorities will be required to upload the data received from PSPs in an EU central electronic repository, to be developed and maintained by the European Commission. This data repository will be available only to the EU Member States in the framework of Eurofisc. Officials of the European Commission will have access to the system only for maintenance and development purposes. The data will be retained in the central repository for an interval of two years. Then they will be erased. The storage period in the central repository is shorter compared to the ten years foreseen at national level for tax authorities in order to reduce the volume of information to be stored in the central repository.

The central repository will allow the "search" function (like sub-option 3.1) and will also automatically aggregate data per payee. It means that the central system will aggregate all payment data received by all payment service providers established in the EU referring to single payees, will be able to recognise multiple records (from different payment service providers) on the same payment transactions. Furthermore, based on indicators chosen by the Eurofisc officials, can retrieve from the system transactions over a given amount, or frequent multiple payment transactions per payee, or per country etc... Finally the system will have a cleansing function: the system will recognise any

¹²⁵ The legal base is in Chapter X of Council Regulation (EU) 904/2010 on administrative cooperation and fighting fraud in the field of VAT.

¹²⁶ See Annex 12 "Visual examples of the regulatory options".

inconsistency or mistake in the format of the data and will "clean" it, learning also from the past.

The software will work based on criteria for the selection of the payees established jointly by the Eurofisc officials of the Member States. The central repository will be able to aggregate the data per payee based on the information available from all the Member States. Under this sub-option the risk analysis will be carried out jointly by the Eurofisc officials in the framework of the Eurofisc network. In this way they can obtain an EU wide view of the VAT fraud schemes.

Finally, like in sub-option 3.1, based on the risk analysis the Eurofisc officials will have to activate their own tax administration to crosscheck data with other national sources of intelligence.

5.5. Discarded option

5.5.1. VAT split payment

A split payment mechanism would change the regular VAT collection regime by introducing on payments for taxable supplies a split between the VAT amount and the taxable base (e.g. by two separate payments for every taxable transaction). It deviates from the current EU VAT regime, which mainly relies on vendor-based collection of VAT and on periodical reporting and payment of VAT by registered traders. The split payment is regarded as a measure that can combat VAT fraud and non-compliance by removing the opportunity of suppliers to charge VAT and disappear without declaring or paying it to the tax authority. A Deloitte study¹²⁷ measured the impact of the general application of the split payment in the EU on the current VAT regime including on B2C supplies. The study concluded that the benefit in terms of reductions in the VAT Gap are not unequivocally higher than the costs imposed on businesses and public bodies (both administrative costs and cash flow impacts), and are even outweighed when applied to the entire volume of transactions. Furthermore, in order to apply the split payment of the VAT amount the payment service provider should be aware of very detailed and specific information in order to determine exactly the VAT liability. The collection of this information is considered technically highly challenging under the SEPA regulation and the PSD2.

5.5.2. Direct access of Member States' tax authorities to Payment Service Providers' databases

Another technical solution to give Member States the access to payment data would be through a direct access of tax authorities to PSPs' databases. However, this solution is considered disproportionate in terms of processing of personal data. In fact, not all payment data are necessary for tax authorities to achieve the objective of fighting e-commerce VAT fraud. In particular data on domestic payments would not help to detect cross-border transactions. Finally the data on payers are disproportionate in terms of data protection, because would disclose information on the consumers that are not necessary for tax authorities. Therefore, this option has been discarded.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

6.1. Methodology

An evaluation of Council Regulation (EU) 904/2010 was undertaken with specific regard to e-commerce VAT fraud. A public consultation and a targeted consultation with tax

¹²⁷ See: https://ec.europa.eu/taxation_customs/sites/taxation/files/split_payment_report2017_en.pdf

authorities and business representatives were launched in the first half of 2018. The outcome of the consultations, and in particular the answers and estimates provided by tax authorities and business have been taken into account. The evaluation is annexed to this report.

6.2. Analysis of the impacts

Nature of the analysis and factors affecting it

It was not possible to carry out a quantification of the impacts of this initiative through a CGE (computable general equilibrium) model simulation in the time available. The analysis of the impacts will therefore be laid out essentially in qualitative terms. While this is not optimal, it must be considered that the effective impact of this initiative, for reasons that will be explained in detail later, will depend to a large extent on a) the scope and pace of implementation by individual Member States of new control protocols b) the quality, degree, and timing of administrative cooperation between Member States and, c) the degree by which third country jurisdictions cooperate in enforcing EU VAT law. Given that these three parameters are very hard to forecast, any quantification of the impacts would at any rate be subject to a large error margin. The analysis mainly addresses the economic impact of the options, administrative and compliance costs for stakeholders, and the impact on the fundamental rights to protection of personal data. Social and environmental impacts are shortly addressed: a more detail analysis of these impacts was not possible due to the very technical nature of the options.

Key Assumptions

1. *Continued growth in e-commerce:* The trend towards an increasing volume of e-commerce is expected to continue as more and more consumers familiarise with purchasing over the internet. While the rate of growth of e-commerce is likely to continue moderating as the sector matures¹²⁸, there is general consensus that this trend will continue. The growing concerns about the protection of personal data are assumed not to change this outlook fundamentally; the indications from stock markets, which are by their nature forward-looking, corroborate this assumption¹²⁹.
2. *Increasing adoption of payment control tools by national tax administrations:* At national level, it is assumed that in the medium term more tax administrations will seek to introduce payment control tools, on account of the successful experience of countries like Norway, Australia, and several EU Member States (see section 5.2). For the assessment of the impacts, it is also assumed that tax administrations adopt the flanking measures needed to ensure the effectiveness of the payment control tools; in particular, that they allocate sufficient staff to carry out the checks on the suspect traders identified thanks to the new tools.
3. *Further reinforcement of cooperation between EU tax authorities:* The effectiveness and quality of cooperation between EU tax administrations is assumed to improve further because of multiple ongoing policy initiatives to address VAT fraud and because of a more propitious political climate.

¹²⁸ Source Ecommerce Europe Report 2017

¹²⁹ From 1.1.2014 to 31.10.2017, the return on Amazon stock was +262%, compared to a 44% loss for traditional retailers. The general SP500 index returned +28%. The gap between Amazon and traditional retailers continued to grow in 2017 (see <http://uk.businessinsider.com/amazon-stock-price-retail-apocalypse-2017-11?r=US&IR=T>). The same general trend is expected in the EU, where the share of enterprises selling online has grown from 13% to 18% in the five years to 2016, and worldwide.

4. *Increased collaboration with third country tax authorities:* Finally, it is assumed that third country tax administrations will increasingly collaborate with EU tax authorities in the enforcement of VAT rules on B2C sales on EU territory. As pointed out in the problem definition, currently some important players do not cooperate with the EU in enforcing VAT payments on B2C businesses on account of exclusions stipulated in the OECD framework. However, the OECD is very active with the BEPS initiative in order to improve international cooperation also in the field of consumption taxes¹³⁰. Furthermore, China has recently introduced a new VAT system¹³¹ following the OECD guidelines: it is reasonable to expect further steps also in the field of international cooperation (jurisdictions with similar consumption tax systems based on the destination principles tend to cooperate for the assessment of VAT liabilities). Overall, it is assumed here that, as the policy options outlined in this initiative lead to a greater awareness of the e-commerce VAT fraud and to identification of the fraudsters located in third-country, changes will be made to the collaboration framework that lead to significantly greater pressure on dishonest businesses also in third countries.

Assumptions 1 to 3 are deemed to be fairly straightforward and it seems difficult at present to imagine any markedly different scenario, so that they will not be further discussed. For assumption 4, given that it depends on the actions and policy of third countries, we present – alongside our central scenario – an alternative 'non-cooperation scenario' when discussing the impacts on fraud and on trade distortion¹³².

6.2.1. Impact on VAT fraud

General considerations

The judgement that payment data availability represents a quantum leap in the effectiveness of the fight against e-commerce VAT fraud is not merely a prospective opinion but is borne out of an understanding of the antifraud controls in current administrative practice. Already now, as outlined in the problem definition, the EU administrative cooperation framework allows tax administrations to retrieve information about businesses operating from other EU jurisdictions, if any wrongdoing is suspected. Information and transactions data can be sought not only from the tax administrations of other Member States, but – in some case – even from payment intermediaries themselves. However, for legal reasons related to data protection and due process, such information is normally available only on the basis of a *targeted* and *duly motivated* request, while a general 'screening' data request would be immediately refused. In other words, once a tax administration has identified a trader as suspect, existing tools can be quite effective in enforcing the VAT (at least in the case of an EU-based suppliers).

However, the problem which existing cooperation agreements do not allow is how to effectively identify suspect businesses in the first place. Existing systems rely mainly on checking parcels or on follow-up work done on regular VAT audits. This approach could suffice when the volumes of cross-border B2C sales was limited. However, the exponential growth in e-commerce implies that a system based on controlling parcels would require a very high amount of random checks to provide an effective deterrent to fraudsters. Looking just at small consignments originating from outside the EU, their

¹³⁰ See: <http://www.oecd.org/tax/consumption/oecd-delivers-implementation-guidance-for-collection-of-value-added-taxes-on-cross-border-sales.htm>

¹³¹ See: <https://www.oecd.org/tax/consumption/business-vat-tax-reform-china.pdf>

¹³² We will not discuss the impacts of the non-cooperation scenario on other variables (eg on compliance costs) as they are either not markedly different from the central scenario or straightforward.

number was estimated at 115 million already in 2013¹³³, implying that even checking just one percent of packages would require opening more than a million parcels every year. This would require a disproportionate use of human resources.

Given that the control of parcels can only identify a tiny fraction of non-compliant operators, an unscrupulous business can operate at a significant scale with little risk of being discovered by the tax administration of the country of destination of the parcels. Under these circumstances, the main hope for identifying a non-compliant business rests on VAT audits done for other reasons – which can take very long or may never take place. In contrast, the availability of data on payments allows tax administrations to identify which businesses engage in B2C e-commerce and double-check if they are VAT compliant, using IT tools. This streamlines and facilitates enormously the detection of potential fraudsters.

The crucial role of payment data availability in addressing fraud is confirmed by the fact that more and more tax administrations are adopting this approach. At present, twelve tax administrations already cooperate with PSPs to collect payment data or have put in place payment data monitoring.

The experience of the Finnish tax administration can provide some elements to assess what can be the quantitative impact of introducing payments data to track down non-compliant B2C sellers. In the three years from 2015-2017, the use of payments data was key in the initiation of about 300 audits, with a growing trend. These audits allowed assessing a total of over EUR 29 million. Data for 2016, the year where the amount revealed by the audits was highest; indicate that around 90% of the audits referred to distance sellers. That year, the VAT collected after the audits raised around EUR 16 million Euros. The Finnish tax administration thus gives us an example of why the use of payment data was important in recovering amounts owned by taxpayers. Consequently, payments data analysis is reported to be the key tool to tackle e-commerce VAT fraud.

In the targeted consultation, almost three times as many Member States answered that new tools are needed to effectively address e-commerce fraud than those that considered existing tools sufficient. Others, however, pointed out that an impact on fraud is expected from the new measures introduced in the VAT Directive by the VAT e-commerce package)¹³⁴ and that the impact of these should be seen before judging.

*Comparison with the measures introduced with the VAT e-commerce package and the regulatory option*¹³⁵

Overall, the analysis conducted in the context of this Impact Assessment suggests that the impact (in terms of fighting e-commerce VAT fraud) of the options envisaged under the payments initiative on combating fraud would go well beyond the impact of the measures introduced by the VAT e-commerce package and described in section 5.1, strengthening it in significant ways. This assessment rests in particular on the following considerations:

- The measures envisaged in the regulatory option cover a significantly larger scope than the measures included in the VAT e-commerce package; in particular, as described in section 5.1.4, while the deemed supplier provision covers only certain internet platforms and only for certain supplies of goods, the regulatory options cover all PSPs established in the EU which deal with more than 90% of online B2C supplies of goods and services, making it very difficult to escape detection;

¹³³ See Table 2 on page 35 in *Assessment of the application and impact of the VAT exemption for importation of small consignments*, study prepared for the European Commission, EY – May 2015, available at https://ec.europa.eu/taxation_customs/sites/taxation/files/docs/body/lvcr-study.pdf

¹³⁴ See section 1.1 and section 5.1.

¹³⁵ See Annex 13 " Comparison amongst different initiatives in terms of fighting e-commerce VAT fraud"

- The measures introduced by the VAT e-commerce package are targeted to specific transactions, i.e. the abolition of distance sales thresholds apply only to intra-EU supplies, the IOSS and the abolition of small consignments exemption apply only to imports, the deemed supplier provision applies only to supplies of goods). The envisaged measures under the regulatory option (and partially option 2) will allow a control to all cross-border supplies to final consumers.
- The measures envisaged in the regulatory option (and partially option 2) will be more effective, because they introduce additional elements: in particular, they lay the groundwork for addressing the identification problem (of not VAT registered suppliers), whereby national tax administrations may remain unaware of fraudulent activity by an operator because of legal limitations to existing data exchange procedures. Furthermore, payment data when cross-checked with VAT data will give an important indication of whether VAT declarations are submitted and correct (in terms of turnover declared). Moreover, mis-description of imports (i.e. “gift” or “low-value samples”) will be easily spotted by cross-checking payment data. Finally, the origin of the payments will support tax administrations in their task of checking whether the VAT is declared in the right place of consumption (i.e. where the buyer is located).
- The measures introduced with the VAT e-commerce package will enter into force in 2021 and it is still premature to make a real assessment. However, as already mentioned, they are mainly “simplification” rather than anti-fraud initiatives, although simplification measures to some extent should also improve “compliance”. On the other hand, payment data will help to detect VAT fraud (intentional non-compliance) and also non-compliance (non-intentional) once crossed-matched with VAT declarations.

In particular, Options 2 and all sub-options of Options 3 are expected to have a significant to large impact on reducing **intra-EU fraud**. The impact is largest under option 3.2, because the central repository, by making possible the pooling of EU-level data, will allow to aggregate data over all EU Member States. This is essential for controlling the respect of the EU wide VAT thresholds described in section 5.1.1.

Option 2 is assessed to be less effective than Options 3.1 and 3.2; while adoption of guidelines may speed up adoption in some cases, as Member States with less administrative capacity can rely on the guidelines instead of developing their analysis *ex nihilo*, experience in the taxation domain shows that guideline writing can in itself be a slow and complicated process. Furthermore, non-binding guidelines and the associated non-coordinated adoption of payment data analysis do not merely likely slow down adoption but also aggravate the risk of perverse incentives, exacerbating market distortions (see next section).

As for e-commerce VAT fraud by **extra-EU suppliers**, under the assumptions laid out at the beginning of this chapter, the policy options under consideration are assessed to provide, in the medium term, a positive impact on fraud levels. The effectiveness of the options will be, however, less on extra EU suppliers than on intra-EU suppliers because within the EU, the existing administrative cooperation framework offers a series of tools to recover unpaid VAT in another jurisdiction; whereas, in comparison, administrative cooperation with non-EU tax authorities is in an embryonic state and does not yet guarantee an effective and credible recovery of unpaid VAT, as explained in section 1.3. Note however the discussion of the risks of trade diversion in section 6.2.2.

Risks stemming from lower than expected collaboration from third country jurisdictions

As outlined under assumption 4, it is assumed that availability of data on fraud will trigger greater collaboration with third countries authorities, because of higher awareness

in EU countries and because third countries tax authorities, too have an interest in maintaining a good working relationship with foreign tax authorities in general and with the EU in particular. Given the importance of the EU on the world stage, it seems unlikely that foreign tax authorities would find a non-collaboration strategy sustainable in the long term, although it has to be recognised that in the short term, non-collaboration is a possibility.

The existing level of administrative cooperation with third countries should not be taken as a given, because, if the payment data initiative is adopted, this will in itself give a strong impetus to conclude new, stepped up cooperation agreements. This is because the higher awareness provided by data and the transparency about transactions at risk of VAT fraud will inevitably create a significant pressure for upgrading existing cooperation frameworks. The situation will be markedly different from today's status quo in which there is very little certainty about the size and existence of fraudulent transactions. As such, the level of cooperation with third countries should not be treated as *exogenous* to the policy options, but is to a large extent endogenous (dependent) on them.

Overall, we conclude that both policy options would have a positive impact on reducing e-commerce VAT fraud; this effect would be significantly stronger for the two sub-options of option 3; in addition, the impact on intra-EU transactions would be stronger than on extra-EU transactions, but would be positive for both.

Non-cooperation by third-country jurisdiction would have two main negative impacts: first, it would reduce the positive impact of the policy options on VAT revenue; second, it could trigger trade diversion as businesses might concentrate their operations in non-cooperative jurisdictions. The second impact appears to be the more serious of the two, because about 80% of cross-border e-commerce sales originate from other EU countries, whereas a shift in the market towards third-countries would create more lasting damage.

Despite the risk of non-cooperation outlined above, we expect for the medium/long term a positive impact of the envisaged policy options is nevertheless expected even with respect to traders located in countries where no cogent enforcement framework is put in place. This assessment is based on three sets of arguments: Psychological and reputational considerations; the risk of blocking of non-compliant traders' web pages by tax authorities, and the possibility for tax authorities to introduce additional measures targeting non-compliant non-EU businesses.

a) Psychological and reputational considerations encourage in particular larger traders to be compliant

It is known from the literature on behavioural economics that economic agents tend to comply with tax rules more than they would rationally be expected to do solely looking at the risk of detection and the prospect of a financial penalty¹³⁶. As such, the mere introduction of a scheme to collect data on B2C at EU level seems likely to spur greater compliance than is presently the case. Furthermore, while many smaller traders may not be overly concerned by the reputational damage they might incur if charged with VAT fraud, it seems likely that platforms operated by large, well-known multinational businesses, which play an important role in the e-commerce market, would not want to see their name associated with systematic VAT fraud, or, even worse, to be accused of facilitating VAT fraud. Thus, pressure for voluntary compliance would certainly increase

¹³⁶ See for instance discussion in A. Leicester, P. Levell, I. Rasul, " Tax and benefit policy: insights from behavioural economics", IFS Commentary C125, Institute for Fiscal Studies, London, 2012, p. 82 ff.

once businesses become aware that authorities have ways to detect VAT fraud and non-compliance, even in the absence of a cogent and operational enforcement mechanism.

b) Persistently non-compliant traders face a risk of blocking of web pages

A number of administrations have indicated¹³⁷ that they are legally empowered to block, on their territory, the operation of web pages associated with wrongdoing, and that in the case of persistent violations, this tool could be used to sanction non-compliant foreign suppliers. While, faced with such a sanction, a foreign supplier might open another website, it seems that this would inevitably result in the loss of some business as clients would no longer be able to place their orders on the customary website and would have to identify the new web page through a new search, or following a link to a new page sent by the vendor, both of which processes are likely to result in some leakage.

The deterrent effect of such sanctions would probably vary considerably from one supplier to the next, because of different demand price elasticities; the experience with sites streaming audio-visual content suggest that blocking sites can have a limited effect in cases of a very high price sensitivity and where the content is an e-service. However, in most cases one can believe that businesses would view the potential disabling of web pages as a significant problem and that this is likely to induce greater compliance. Basing on payment data statistics, national authorities would also be able to roll out such sanctions in a more effective manner. Therefore, overall one can conclude that the combination of greatly enhanced detection thanks to availability of payments data, coupled with the threat of blocking the supplier's site by the tax authority is likely to have an impact on reducing extra-EU e-commerce VAT fraud even in the absence of strong cooperation mechanisms between the EU and the country of establishment of the supplier.

c) Member States could introduce additional, specific measures to target non-compliant third country businesses

In case of persistent non-collaboration by third country jurisdictions, Member States could introduce specific measures. Member States could for example require, non-EU businesses to appoint a local VAT representative with joint and several liability or impose joint and several liability on online marketplaces for unpaid VAT on goods sold through the website. These measures would be significantly more effective once it is coupled with payments data information, than it is at present.

Impacts on fraud volumes, by option

Table 3 presents the expected impacts of the options on fraud volumes side by side to facilitate comparison. Option 1 is not included because it is the status-quo option.

Option 2

This option consists of developing voluntary guidelines for Member states to facilitate introduction of payment data tools and coordination between EU tax administrations. This option is assessed to have a modestly positive impact, because it will speed up adoption of payment data tools by tax administrations and will reduce its costs thanks to better sharing of know-how; the impact will depend on how many Member States adopt these tools. However, adoption will likely be gradual; thus, this option implies that the EU will not be able to collectively exert pressure on third countries to enter into

¹³⁷ See section 5.3.1

cooperation agreements. As such, the impact of this option on non-EU traders would be rather limited.

Option 3.1

Compared to option 2, this option would imply a simultaneous introduction of the tool throughout the EU; the coordinated adoption of the tool would also allow better cooperation between EU tax authorities. Both of these aspects would correspondingly create a stronger deterrent effect for fraudsters. This option is thus expected to result in a sizeable reduction of fraud levels and a greater reduction of fraud than under Option 2.

As for non-EU fraudsters, the impact would be less strong owing to the fact that administrative cooperation agreements with third countries are now at an incipient stage, compared to the EU. However, availability of data from all EU Member States would facilitate collective action to improve administrative cooperation agreements with third countries. As such, this option is expected to result in a perceptible decrease of fraud over the medium to long-term in our central scenario. In the alternative non-cooperation scenario, where no effective agreements with third countries are struck, the expected impact would be a limited reduction in extra-EU fraud levels. In theory, fraud levels could even increase in case of strong trade diversion (see also next section) but this would require a rather implausible set of assumptions (high demand and supply price elasticities, absence of reputational effects, ineffectiveness of countervailing measures by Member States, on top of the non-cooperation hypothesis which is in itself not a likely outcome).

Option 3.2

This option has the strongest effect on fraud levels as its centralised nature fosters cooperation more effectively and makes data analysis more efficient because of easier data pooling. The impact on extra-EU fraud is similar to that of option 3.1, with a slightly stronger effectiveness compared to option 3.1 because of easier cooperation (under the central scenario).

Table 3 Fraud levels: net impacts over baseline, by option

Scenario	Location of traders	Option 1 (status quo) Baseline	Option 2 Voluntary guidelines	Option 3.1 Distributed application	Option 3.2 Central storage
Central scenario	EU traders	VAT fraud volumes increase. From 2021, impact of the VAT e-commerce package measures may reduce growth of VAT loss volume	+	++	+++
	Non-EU traders	VAT fraud volumes increase. From 2021, impact	0/+ Negligible to limited: a patchwork-like	+ /++ While enforcement will depend on	++ Similar impact as 3.1, but greater

		of the VAT e-commerce package measures may reduce growth of VAT loss volume	adoption will limit coordinated action vs. third countries	third country cooperation, increased detection expected to result in positive impact through spontaneous compliance and by stimulating adoption of international agreements	transparency and cooperation expected to result in stronger effects
Non-cooperation scenario	EU traders	as above	0/- Under non-cooperation, there might be a tendency for fraudsters to concentrate in Member States with a low effectiveness of controls	+ /+++ Given EU institutional setup, payment data availability would have a positive impact even under sub-optimal cooperation	+ /++ Given EU institutional setup, payment data availability would have a positive impact even under sub-optimal cooperation
	Non-EU traders	as above	0 Lack of collective EU action will limit incentives for third countries to cooperate	? There might be increases in fraud in non-cooperating jurisdictions; nevertheless, fraud may decline at larger traders due to reputational concerns and flanking measures. Final effect uncertain	? There might be increases in fraud in non-cooperating jurisdictions; nevertheless, fraud may decline at larger traders due to reputational concerns and flanking measures. Final effect uncertain

Legend: 0: negligible impact; + (-): limited positive (negative) impact; ++ (++): sizeable positive (negative) impact; +++ (---) strong positive (negative) impact

6.2.2. Impact on distortion of competition

The level of distortion of competition is in direct relation to the level of e-commerce VAT fraud: the greater the VAT fraud, the greater also the distortion of competition. As such, we can expect the following main trends:

- Under the *no-policy change option* (Option 1), distortion would increase following the expected higher volumes of e-commerce. There is even some likelihood that VAT fraud levels increase more than proportionately as businesses gain experience with e-commerce and conclude that existing instruments to fight fraud are inefficient and through the typical learning activity by fraudsters. The impact of this would be uneven across sectors; for example, e-commerce fraud is likely to be more prevalent amongst vendors of price-sensitive, commoditised goods. It is also to be expected

that extra-EU fraud will grow more than proportionately to intra-EU fraud because the stronger existing cooperation between EU tax authorities has a deterrent effect.

- However, the entry into force in 2021 of the deemed supplier provision¹³⁸ could result, in a number of additional impacts. It should be noted that the provision affects only e-commerce platforms. While the provision in itself could lead to a reduction of the rate of growth of e-commerce fraud, unscrupulous businesses could decide to operate outside of e-commerce platforms affected by the deemed supplier provision.

The fact that the deemed supplier provision applies only to part of the market, i.e. e-commerce platforms, create a potential for distortion, as unscrupulous vendors might move out of regulated platforms to continue avoiding VAT. It is difficult to assess, as things now stand, how strong the distortionary impact of this partial coverage of the market could be, because implementing provisions are only now being drawn up and no impact assessment was carried out. It might be limited initially, given the important role of platforms in e-commerce; platforms are important for generating trust among consumers, which is a key prerequisite for e-commerce. However, as time goes on, it cannot be excluded that the impact could grow to be significant, as a roughly 20% potential for price differences is not negligible, particularly for certain commoditised types of goods for which the price elasticity of demand is high.

Overall, under our assumptions, the impact on market distortion would be positive and will mirror the projected reduction in intra-EU and extra-EU fraud determined by option 2 and particularly option 3. An important assumption in this respect is that the introduction of payment data monitoring is followed by EU initiatives to strengthen cooperation with tax authorities in non-EU jurisdictions (assumption 4 above); if no initiatives in this regard are adopted, the risk of trade diversion increases significantly (see discussion in next section)

Risks

- As discussed in the previous section, the main risk would be either that business is diverted to websites operated directly by suppliers outside the EU, or that entire platforms are set up out of the EU and operate in such a way as to escape cooperation with EU tax authorities. The reasons why this risk, although recognised, is not considered the central (i.e. most likely) scenario are listed in section 6.2.1. The risk of trade diversion is higher under the non-cooperation scenario.
- Within the EU, trade distortion should decrease, under our assumptions, as the more effective control allowed by payments data monitoring shrinks the areas in which fraudsters can operate. In this context it should however be mentioned that an uncoordinated approach to use of payments data within the EU could increase the potential for distortion by magnifying perverse incentives; this is because the more numerous are countries effectively fighting e-commerce VAT fraud, the greater become the benefits for fraudsters installed in non-cooperative jurisdictions. This is why the effectiveness of the options involving greater coordination, viz. the two sub-options under option 3, is greater, as it counteracts the risk of administrative inertia. This however also raises a potential risk that some jurisdictions do not follow the ‘loyal cooperation’ rule stipulated under the EU treaties but remain relatively inert in hopes of attracting B2C business to their country. In that case, which does not represent the central assumption in the analysis, obviously, fraud might concentrate in

¹³⁸ For the deemed supplier see section 1.1 and section 5.3.1. There is no certainty yet on the operational implications and on the impact of art. 14a as this was introduced in the directive during negotiations in the Council and as a result was not subjected to an impact assessment. Furthermore, the implementing provisions are only now being developed.

some jurisdictions, reducing the positive impact from the measures taken. Overall it seems unlikely however that this phenomenon reaches systemic proportions, given the reputational costs of such a strategy and the current societal low tolerance for VAT fraud.

The same diversion risk affects also extra-EU trade, particularly in the non-cooperation scenario. Traders might concentrate their operations in jurisdictions where there is no, or limited, cooperation with EU tax authorities in recovering due VAT. As mentioned in the section on VAT fraud, even in the absence of administrative cooperation, factors such as reputational concerns or the threat of website blockage work to counteract wilful fraud, once authorities have detected non-compliance. Nevertheless, the risk that for certain market segments, trade diversion out of the EU increases cannot be excluded. The higher level of this risk for extra-EU jurisdictions explains why the effectiveness of the proposed measures is rated higher for intra-EU e-commerce. Finally, a strong increase of trade diversion, particularly in a non-cooperative scenario, could also jeopardise the attainment of the objective of reducing overall VAT fraud.

Distortion of competition: net impacts over baseline, by option,

Scenario	Location of traders	Option 1 (status quo) Baseline	Option 2 Voluntary guidelines	Option 3.1 Distributed application	Option 3.2 Central storage
Central scenario	Intra-EU traders	Market distortion to increase in line with VAT fraud volumes From 2021, deemed supplier provisions may exacerbate risk of diversion	0/- Different levels of adoption and the resulting different intensity of combat against VAT fraud could increase perverse localisation incentives	++ A more effective detection and enforcement will reduce intra-EU market distortions	+++ Similar to 3.1, but effect enhanced by expected better cooperation
	Extra-EU traders	Market distortion to increase in line with VAT fraud volumes From 2021, deemed supplier provisions may exacerbate risk of diversion Aggressive enforcement of intra-EU provisions may exacerbate risk of diversion	0/+ Limited Stepped-up enforcement in only some EU countries will result in a limited (under the assumption of cooperative behaviour) or negligible reduction of trade distortions vs non-EU countries	+ / ++ Impact will be in line with reduction of VAT fraud on extra-EU transactions	++ Impact stronger than in 3.1 as this option is expected to foster more effective coordination vs. third countries
Non-cooperation scenario	Intra-EU traders	No big difference from central scenario given limited scope of current cooperation agreements with third countries	- In a non-cooperation scenario, stepped-up enforcement in only some EU countries could result in some increase in trade distortions	+ Availability of payments data will increase pressure for effective tracking down of non-compliant firms.	+ / +++ Availability of payments data will increase pressure for effective tracking down of non-compliant firms. Centralised system will increase

					effectiveness.
	Extra-EU traders	No big difference from central scenario given limited scope of current cooperation agreements with third countries	-- In a non-cooperation scenario, stepped-up enforcement in only some EU countries could result in some increase in trade distortions	--/--- If no action is taken to ensure third-country cooperation, there is a risk unscrupulous traders concentrate their operations in extra-EU jurisdictions.	--/--- If no action is taken to ensure third-country cooperation, there is a risk unscrupulous traders concentrate their operations in extra-EU jurisdictions.

Legend: 0: negligible impact; + (-): limited positive (negative) impact; ++ (---): sizeable positive (negative) impact; +++ (---) strong positive (negative) impact

6.2.3. Impact on administrative burden and compliance costs

Introducing new obligations to supply data (for PSPs) or exchange them (for tax administrations) can, generally speaking, create costs for operators. These costs fall under two categories: set-up and learning costs, which are incurred once only when the new system is introduced, and running costs. These costs have been assessed relying mainly on Commission IT cost assessments but also on input from Member States' tax administrations and the replies of stakeholders to the targeted and public consultations.

a) One-off costs

The Commission services made a first assessment of the capital costs for setting up an IT infrastructure for monitoring payments data for Member States and for the European Commission (see Table 4). This estimate is based on an extrapolation of the costs from the Customs Information System¹³⁹ rather than on a feasibility study and as such should be considered a prudent, de maximis estimate (indeed, some Member States which have set up a payments data monitoring system have indicated that they incurred a lower level of costs).

In both option 3.1 and option 3.2 Member States will have to collect payment data in a national database. Then, the distributed system consists in an electronic interface that will connect the different national databases and will allow the officials of one Member State to “interrogate” the systems of the other Member States. The centralised system will just collect all payment data that will be transmitted by the Member States. In the distributed system different functions will be decentralised and, thus, more expensive for Member States to develop and maintain (i.e. the cleansing of the information received from payment data), training, hardware, information dissemination costs. These costs will be bare by the 28 Member States under the distributed application, while only once under the central system.

Such capital costs ('CAPEX'), which can be seen as an approximation of the set-up costs, vary between approximately EUR 221million and EUR 290 million for the EU as a whole – i.e. between EUR 7.5 million (option 3.2) and EUR 10.3 million (option 3.1) per Member State, and EUR 1.8 million (option 3.1) and EUR 11.8 million (option 3.2) for the Commission. This expense is a one-off cost item that should be amortised over the entire lifetime of the project, which, on the basis of prior experience, can be estimated at

¹³⁹ The Customs Information System is a central database managed by the Commission for Customs controls.

10-15 years at a minimum. Thus, an amortisation rate in the environment of EUR 0.7 million per annum for each Member State is a balanced maximum estimate.

The Commission estimates also indicate that cost wise, option 3.2 is the best, while option 3.1 is somewhat more expensive, although the difference is not very significant. Option 2 is found to be less expensive than the others because it does not include the cost of any individual system set up by the Member State; in reality however the comparison should more properly be made with the cost of setting up a system on a national basis, which seems likely to be more expensive as this approach would limit the gains from economy of scale.

Table 4: Total Member State + EU Commission costs for payments data IT infrastructure (EUR million; rounded)

	CAPEX (Total, EU28 + Commission)	CAPEX (per Member State)	CAPEX (Commission)	OPEX (5-year total, EU28 + Commission)	OPEX annual average (per Member State)	OPEX annual (Commission)
Option 2	0.2	-	0.2	0.15	-	0.03
Option 3.1	290	10.3	1.8	550	3.9	0.96
Option 3.2	221	7.5	11.8	429	2.9	4.5

Source: Commission services preliminary estimate

As for private businesses, the main impact would be on PSPs, who under the various options would have to materially put the data at the disposal of the authorities. The stakeholder consultation has however revealed that, for these entities, existing IT systems could be used – or adapted at a moderate cost – to provide the data, so that the set-up and learning costs would be limited.

b) Recurrent costs

For tax administrations, on the basis of the Commission extrapolation, the running costs ('OPEX') of the IT infrastructure per Member State could be estimated at approximately between EUR 2.9 million (option 3.2) and EUR 3.9 million (option 3.1) per year, not including labour costs to be incurred to exploit these data. The running costs for the Commission would be EUR 0.96 million (option 3.1) and EUR 4.5 million (option 3.2). Similarly to the case of the set-up costs, the overall costs for option 3.2 are somewhat lower than for option 3.1. While the options considered result in a nominal increase in certain costs for the administration, it must be stressed that this allows a substantially greater effectiveness of control activities. The total effect is a reduction of net outlays, as the tax administrations, thanks to data access, carry out audits for larger amounts than the costs incurred by the system. Some Member States have been able to provide data on how many audits were linked to payments data availability and on what amount of VAT was assessed during these audits) (see Table 4)¹⁴⁰. The assessment from these Member

¹⁴⁰ The results showed in table 4 belong to the baseline scenario, where some Member States developed an electronic system to collect, analyse and use for control purposes payment data in a systematic way, while other Member States do not have such a system and, thus, the results in terms of additional VAT collected and assessed are limited. The consultation with Member States showed that only 50% of the Member States collecting payment data at national system have a kind of risk analysis system in place. In particular in some Member States, only payments resulting from the bank accounts are communicated to tax authorities. The EU wide dimension of the information (referring to all kind of payment services resulting in transfer of funds) and the risk analysis within Eurofisc are the main advantages that will bring higher benefits and a full EU picture to all Member States.

States was that the benefits offset the costs (see the replies to the public consultation for more details..

Table 5 Audits for which the use of payments data was important

	Year	2015	2016	2017
	Member State			
Number of audits	Finland	46	145	104
	Slovenia	NA	NA	25
VAT assessed (EUR thousand)	Finland	2.176	23.168	3.671
	Slovenia	NA	NA	136
VAT collected (EUR thousand)	Finland	NA	16.569	NA
	Slovenia	NA	NA	NA

Source: Targeted consultation

Pooling the data from all available audits, we arrive at an average value of VAT assessed per audit (in cases where the use of payment data was important) of slightly above EUR 90°000 per audit. While this average reflects a high value for 2016, a comparison with annual running costs incurred by the Finnish tax administration of around EUR 100°000 suggests that, if tax administrations utilise the payments data to step up audits, completing a relatively limited number of additional audits will suffice to cover costs; although the costs for a comprehensive EU system will be higher, it will also be more effective. Scale considerations too suggest that the amounts of potentially recoverable VAT dwarf system costs (see box below). We conclude that the *net* cost of the payment data system is negative. As such, control costs are assessed to be *reduced* by the options being considered, despite the fact that they require some budgetary outlay to be started.

What is the order of magnitude of recoverable VAT?

Although it is very hard to estimate fraud levels, there are solid grounds to believe that there are ample margins for increasing revenue from a more effective control of e-commerce. Member States' tax administrations agree that fraud levels, even in intra-EU business, are significant owing to the current unsatisfactory effectiveness of controls. The order of magnitude of the amounts at play can be assessed by looking at the total annual value of B2C e-commerce. Even not considering extra-EU suppliers, B2C web sales accounted for around EUR 600 billion in 2017¹⁴¹. Each 1% of fraud on turnover would therefore generate, at EU 28 level, up to EUR 1.2 billion in non-assessed VAT. Even accounting for incomplete recovery of assessed VAT, these amounts exceed the

¹⁴¹ E-commerce Europe estimated the 2017 e-commerce turnover at EUR 602 billion for the North, East and South region of Europe for 2015.

operational costs for the entire EU. Furthermore, fraud levels likely account for several percentage points of e-commerce sales.

Looking at compliance costs for payments service providers, they currently receive data requests in different formats and following different procedures, which then requires from them substantial work to comply. Compliance further exposes PSPs to legal hazard because of the different regimes for data protection. While it was not possible to quantify the costs of the different options based on the result of the targeted consultation¹⁴², the strong preference of PSPs for a harmonised solution indicates that the cost saving effect compared to a non-coordinated approach can be substantial. In addition, the number of data requests can be expected to grow in the future in line with the expansion of e-commerce. Overall it seems likely that the savings from the ability to supply standardised replies to data requests will more than offset any other recurring cost.

6.2.4. Sectoral impacts

The growth of e-commerce has shown that over time, consumers may extend their purchases to a greater range of goods over time, as they familiarise with it and become more trustful. Consumers also appreciate the convenience of having a wide range of goods and services at their disposal without having to move. Nevertheless, price competitiveness remains important, as does trust in the vendor. VAT fraud allows vendors to be price competitive¹⁴³ but at the same time consumers prefer sourcing their purchases from reputable businesses operating on well-known platforms that offer them trust and credible dispute resolution mechanisms. The need to sustain consumer trust will continue to be a potent force limiting the propensity of consumers to seek savings from suppliers operating outside established portals. This means that it is inappropriate to extrapolate any impact directly from the level of e-commerce in particular sectors, as the fraud rate is likely to vary substantially between sectors and even within the same sector. Given the above dynamic balance between sensitivity to price and need for trust, the risk of VAT fraud and market distortion is highest in highly price-sensitive, commoditised markets. Many of these markets are already now dominated by extra-EU vendors. Another area where price sensitivity is relatively high, and where as a result there is a high risk of evasion and distortion, is streaming of audio-visual content over the internet. Greater control of VAT fraud is therefore likely to have varying effects on trade patterns; while the sourcing of commodities, low-cost goods is unlikely to shift much trade, higher-value goods for which trust and consumer service are important should see a reduction of competition from unscrupulous businesses and from extra-EU competition. This should result in improvements in EU competitiveness in certain markets. The size of these effects will be highly dependent on the nature of the individual goods and services traded.

Impact on prices

The impact on prices will depend on the price sensitivity of the individual goods or service and on whether it can be sourced from non-cooperative jurisdictions. In the extreme case of a good with high price sensitivity, produced by a perfectly competitive sector located in a non-cooperative jurisdiction, the impact on prices would be negligible and trade would be diverted towards the non-cooperative jurisdiction. In the more normal

¹⁴² One contribution was received from a stakeholder with an indication of a recurrent cost impact of 100.000 euros annually. However, this is not felt to be a good basis for analysis because it lacks sufficient detail and seems not to take into account offsetting savings on data requests.

¹⁴³ See annex 7, Case study – pricing policy and estimation of potential VAT loss

case of a good produced by a business enjoying a degree of market power and facing some positive incentives towards tax compliance, theoretical considerations on tax incidence suggest that part of the higher effective tax burden would be absorbed in the businesses' profit margin and some would be reflected on prices. The degree of price increase would depend highly on the price elasticity of the specific good. Overall, however, the inflationary impact on the general price level is negligible..

6.2.5. Impact on terms of trade, employment and environment

A reduction in the prevalence of fraud on extra-EU B2C supplies would be equivalent to an increase in taxation of imports. This would result in a positive but limited terms of trade effect, unlikely to have any impact at macroeconomic level. Similarly, while there may be sectoral effects on employment, in particular among EU retailers subject to unfair competition, these are likely to be modest or negligible at a macro level. There might be positive but limited environmental impacts linked to transport if there is a reduction in those imports from extra-EU countries that are driven essentially by savings on VAT.

6.2.6. Impact in terms of the fundamental right to protection of personal data

Under the baseline scenario, the tax authorities already collect personal data for the purpose of detecting and fighting e-commerce VAT. Tax authorities' collection, storage and analysis of personal data for taxation purposes imply a restriction to the protection of personal data rights to be regulated by the national law in line with the GDPR. Under the non-regulatory option (option 2), EU guidelines may highlight to the tax administrations the main GDPR rules and relevant jurisprudence.

Under the regulatory option Council Regulation (EU) No 904/2010 on administrative cooperation and fight against fraud in the field of VAT that already lays down data protection safeguards – in line with the GDPR - as regard the storage, the exchange and the use of data under the purpose of the Regulation. The safeguards laid down under Regulation 904/2010 and the GDPR rules will apply to the exchange of payment data under the regulatory option. For the assessment of the necessity and proportionality principles, it should be first noted that the objective of the collection, exchange and analysis of VAT relevant data is the fight against e-commerce VAT fraud. This is well documented by the stakeholders' consultation, where the tax authorities stressed the need of payment data for fighting e-commerce VAT fraud effectively¹⁴⁴. In addition, only the data with a nexus to potential e-commerce VAT fraud will be transmitted to the tax authorities and exchanged between them: in particular only the data necessary to detect potential fraudsters established outside the Member State of consumption (no domestic payments), the amount of transactions that should be subject to VAT, the date of the transactions and the information on where – in principle – the place of taxation should be. The data will only refer to the payees receiving payments from abroad. The data on the payers is not necessary for the objective (apart from the origin of the payment which is necessary to establish the place of taxation) and – thus – not in the scope of the regulatory option. Therefore, the payment data will not be usable – for instance – to monitor the purchase habits of the consumers.

In terms of data storage, an EU central repository (sub-option 3.2) must guarantee the appropriate level of security in line with the rules governing the processing of personal data by the European Institutions¹⁴⁵. While a central repository could be seen as a

¹⁴⁴ See Annex 2, Consultation synopsis report, section 3.2 and section 4

¹⁴⁵ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

potential risk in terms of target for unauthorised access, this is not *per se* a limitation of data protection rules, as long as the confidentiality and security of the data processing is ensured. Indeed, also a distributed application (sub-option 3.1) could be the target of cyber-attacks. Furthermore, there are already EU centralised information systems containing and processing personal data¹⁴⁶. Indeed, both tax authorities and PSPs showed a preference toward a centralised solution.

As for the exchange of data between tax authorities, this will be only within the Eurofisc antifraud officials. Under sub-option 3.1., the exchange of the data will pass through a secured electronic system that encrypts and decrypts the data, and the officials will access the data using personal passwords. Also under sub-option 3.2 the central repository will be accessible only to the Eurofisc officials. Again, this access will be regulated through use of a secure system and personal password and the system will keep track of any access. Furthermore, the data will be retained only for 2 years, in order to allow Member States a reasonable period to carry out VAT audits, and then erased.

Finally, in addition to the exchange of data, the regulatory option also foresees a risk analysis process to focus and narrow down the search to the highest-risk traders. Under sub-option 3.1., this is done nationally while under sub-option 3.2 this is done automatically at European level. However, the two sub-options restrict the access to the risk analysis result of the payment data only to the anti-fraud officials of the Member States' tax authorities in the framework of Eurofisc. The outcome of the risk analysis will have to be further double-checked with other information at disposal of tax authorities (such as VAT, MOSS and Customs information). Only after this process, the result will be used to detect e-commerce VAT fraudsters and carry out VAT controls. Then, as it happens for domestic VAT controls, the taxpayers will be called to confront the information held by the tax authority on which the VAT assessment is ground on, based on the national legislation of the jurisdiction where the taxpayer is established. On the basis of the considerations laid down in the preceding paragraphs, we conclude that the data-sharing measures considered for adoption do not infringe the principles of necessity and proportionality and do not put citizen's and legal persons' data at greater risk of a breach. As such, there is no adverse impact on data protection.

Under both option 3.1 and 3.2 payment data will be processed for operation reasons (VAT controls) by the tax authorities. The GDPR will regulate this process of data, and already foresees safeguards for data protection and restrictions to the scope of the obligations and rights of the data subject. Regulation (EU) No 2018/1725 provides for the same safeguards and restrictions when data are processed by the European Institutions, in this case by the duly accredited officials of the Commission that processes the data for development care and maintenance. In particular, Member States will have to apply the GDPR for the process of data, in their national systems, and for the process of data by Eurofisc officials using the European components of the electronic system. In terms of data storage, an EU central electronic system will guarantee the appropriate level of security in line with the rules governing the processing of personal data by the European Institutions. The system will not have an interface on internet, as the payment operators will submit their information to national authorities. The exchanges of information among national taxation authorities will occur using the secure Common Communication Network, which supports all exchanges of information between taxation and customs authorities and provides to all of them all necessary features for security (including encryption of data). Therefore, in line with Regulation (EU) No 2018/1725 the central system will guarantee by design the highest possible level of data security.

¹⁴⁶ E.g.: the Schengen Information System SIS including the Central SIS II and the Information Customs System.

7. HOW DO THE OPTIONS COMPARE?

7.1. Summary assessment of the impact

Table 6: Summary analysis of impacts

	Option 1 (status quo) Direction of development if no policy change	Option 2 Voluntary guidelines	Option 3.1 Distributed application	Option 3.2 Central storage
Effectiveness of the options				
Impact on VAT fraud (intra-EU)	-- VAT fraud volumes increase. From 2021, impact of the VAT e-commerce package measures may reduce growth of VAT loss volume	+ Limited reduction in VAT fraud in line with speed of adoption	++ Coordinated adoption will speed up update and allows better cooperation	+++ Better suited than 3.1 to monitor threshold; fosters cooperation more effectively than 3.1; better and wider process of data and central risk analysis
Impact on VAT fraud (extra EU)	-- VAT fraud volumes increase. From 2021, impact of the VAT e-commerce package measures may reduce growth of VAT loss volume	0/+ Negligible to limited: a patchwork-like adoption will limit coordinated action vs. third countries	+/ While enforcement will depend on third country cooperation, increased detection expected to result in positive impact through spontaneous compliance and by stimulating adoption of international agreements	++ Similar impact as 3.1, but greater transparency and cooperation expected to result in stronger effects
Impact on market distortion (intra EU)	-- Market distortion to increase in line with VAT fraud volumes From 2021, deemed supplier provisions may exacerbate risk of diversion	-/-- Different levels of adoption and the resulting different intensity of combat against VAT fraud can increase perverse localisation incentives	++ A more effective detection and enforcement will reduce intra-EU market distortions	+++ Similar to 3.1, but effect enhanced by expected better cooperation
Impact on market distortion (extra-EU)	-- Market distortion to increase in line with VAT fraud volumes From 2021, deemed supplier provisions may exacerbate risk of diversion Aggressive enforcement of intra-EU	0/+ Limited Stepped-up enforcement in only some EU countries will result in a limited (under the assumption of cooperative behaviour) or negligible reduction of trade	+/ Impact will be in line with reduction of VAT fraud on extra-EU transactions	++ Impact stronger than in 3.1 as this option is expected to foster more effective coordination vs. third countries

	provisions may exacerbate risk of diversion	distortions vs non-EU countries		
Impact on level playing field for businesses	-- In line with the impact on VAT fraud and distortion of competition SMEs: The increase of market distortion will have a negative impact on EU SMEs which will suffer also from VAT fraud	0/+ In line with the impact on VAT fraud and distortion of competition SMEs: Limited effect In line with the limited impact of fighting VAT fraud	+/ In line with the impact on VAT fraud and distortion of competition SMEs: In line with reduction of VAT fraud and reduction of market distortion	++ In line with the impact on VAT fraud and distortion of competition SMEs: The stronger the impact on VAT fraud and reduction of market distortion, the more level playing field for SMEs
Efficiency of the options				
Impact on tax compliance costs for business * <i>* a positive sign indicates a reduction of costs</i>	- Costs will increase in line with assumed greater volume of data requests from tax administrations	0/+ There may be modest positive effects if tax administration adopt guidelines in a coordinated fashion	++ Standardisation of reporting requirements will sizeably reduce costs in replying to data request from tax administrations	++/+++ Similar to 3.1, but stronger standardisation of operations and software
Impact on control costs for administrations	-- Control costs are assumed to increase to respond more forcefully to increase in VAT fraud volumes and market distortion	+ Administrations can save time and development costs by referring to guidelines	++ Centralised solution would keep down development costs	++/+++ IT costs estimated to be lower than in 3.1
Impact on additional VAT collection for tax authorities	-- In line with the impact on VAT fraud	0/+ In line with the impact on VAT fraud	+/ In line with the impact on VAT fraud	++ In line with the impact on VAT fraud
Coherence with other EU policies				
Coherence with the VAT e-commerce package	-- The simplifications for the compliant businesses are not followed by control tools for tax administration to detect non-compliant businesses	0/+ Limited anti-fraud measures accompanying simplification measures	+/ New anti-fraud tools will facilitate the control of non-compliance	+++ New and more effective anti-fraud tools will facilitate the control of non-compliance
Coherence with the General Data Protection regulation	0/+	++ The EU could disseminate relevant jurisprudence on data protection rules	++ The storage of data will be at national level (GDPR rules will be reflected in national legislation) Exchange of data will be regulated at EU level (GDPR rules will be reflected in the EU legislation)	++ Storage and exchange of data at EU level (GDOR rules reflected in the EU legislation)

Legend: 0: negligible impact; + (-): limited positive (negative) impact; ++ (--) : sizeable positive (negative) impact; +++ (---) strong positive (negative) impact

8. PREFERRED OPTION

8.1. Identification of the preferred option

The analysis above shows that the regulatory option is the one best addressing the specific and operational objectives listed in section 4.2 and section 4.3. Compared to the baseline scenario and option 2 (guidelines) option 3 is the only one ensuring a full harmonisation of Member States' tax authorities' access to VAT relevant payment data. Consequently, option 3 also guarantees the subsequent harmonisation of procedures for risk analysis and – thus – for the identification of fraudsters and to exchange this information at EU level.

In particular, sub-option 3.2 (the central storage) is the one that implies less cost for tax authorities and businesses and ensure the best impact on VAT fraud. While the two regulatory sub-options have a similar impact on VAT fraud, sub-option 3.2 gives more guarantees in terms of uniformity of data and data analysis and – especially compared to sub-option 3.2 (distributed application) – a more clear European view of the turnover of the detected fraudster.

Sub-option 3.2 also has a better impact on reducing market distortion. Where the cooperation brings better results to tax authorities, honest businesses can enjoy of a more level playing field. Compliance costs for businesses (in particular PSPs) are considered lower with the harmonisation of the reporting obligations. This is not the case under the baseline scenario and the non-regulatory option. One single format for the transmission of data and one single interface (sub-options 3.2) reduce the compliance costs of PSPs.

Tax administrations as well bear lower development and running costs under the centralised solution compared to the distributed application (sub-option 3.1) or the non-regulatory option (where they must bear the full investment and running cost of any new IT solution).

In terms of data protection sub-options 3.1 (distributed application) and 3.2 (central storage) are the ones who give more guarantee compared to the baseline and the non-regulatory option because they place the process of payment data under the EU legal framework of VAT administrative cooperation, which already includes specific legal safeguards and secure IT systems to protect the process of personal data.

8.2. Subsidiarity of the preferred option

The preferred option (sub-option 3.2) is considered consistent with the principle of subsidiarity, as the main problem at stake is the e-commerce VAT fraud also triggered by the current tools at disposal of tax authorities to cooperate between them. It has been demonstrated that Member States alone are not able to tackle e-commerce VAT fraud and any initiative to introduce new tools for cooperation, targeted to the specific problem, requires a proposal by the Commission to amend Council Regulation (EU) No 904/2010. New record keeping obligations for PSPs require a proposal to amend the VAT Directive. Therefore, the preferred option clearly offers value over and above what can be achieved at Member State level.

8.3. Proportionality of the preferred option

The preferred option (sub-option 3.2) does not go beyond what is necessary to meet the objective. In particular, the costs are over compensated by the expected return in terms of detection of VAT fraud and additional VAT collection. The administrative burdens for businesses and tax administrations are overall reduced compared to the baseline and other options and the honest businesses will benefit from a more level playing field. Finally, also the process of personal data respects the principles of necessity (only the data necessary to achieve the objective of combating e-commerce VAT fraud are processed) and proportionality (the type of data and the way they are processed by the anti-fraud experts of tax authorities do not exceed the limits of what is appropriate to achieve the objective of fighting e-commerce VAT fraud).

In particular, the initiative is proportionate because – as the report wants to demonstrate – the tax authorities cannot obtain information in other ways. The payment information will not be a duplication of what tax authorities collect through MOSS declaration, or through the platforms under the deemed supplier provision. At the contrary the payment data will be used to cross-check that information. Furthermore, payment data will give the tools to the tax authorities to detect the traders that will be outside the MOSS or not covered by the deemed supplier provision.

The proportionality is also in the kind of data requested to payment service providers: the information they will have to transmit to tax authorities is the information they already have at disposal (PSPs will not have to invest further to collect the requested information).

8.4. Impact on SMEs

For the assessment of the different options' impact, business associations, PSPs and SMEs' associations have been specifically questioned on any specific impact on SMEs. Furthermore, the public consultation has also been circulated within the Enterprise Europe Network¹⁴⁷ in order to receive the highest number possible of SMEs' opinions. Unfortunately, only one SMEs' association replied to the targeted consultation but was not able to indicate whether there are actually SMEs providing payment services that could be impacted by the application of the different options. However, as indicated by the same association, SMEs' in general suffer from the unfair competition of traders exploiting the e-commerce to avoid the payment of the due VAT. Seven respondents to the public consultation were SMEs, some of them e-commerce retailers. They mentioned VAT fraud is damaging SMEs and expressed high expectations in new tools to tackle e-commerce VAT fraud. However, the respondent SMEs did not express any preference for one or another of the policy options and generally could not estimate the impact of those options on SMEs. PSPs and a PSPs association were also asked to indicate figures of the numbers of SMEs in the sector, but they were not able to answer. This is probably because the market of payment services is dominated by large businesses. Anyway, lacking any quantification evidence from the consultation, it is reasonable to assume that any EU harmonisation of reporting requirements will have a beneficial impact on any SMEs providing payment services which, otherwise, will have to deal with different reporting rules and procedure to tax authorities in the Member States. Finally, SMEs in the e-commerce and in the traditional economy will benefit from the more level playing

¹⁴⁷ See: <https://myintracomm.ec.europa.eu/dg/grow/dirunits/H/H1/Pages/thesmetest.aspx>

field whereby Member States' tax authorities will be able to detect e-commerce VAT fraudsters.

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

9.1. Indicators for monitoring and evaluation

The table below give an overview of the objectives, the indicators to measure whether they will be achieved, the tool for monitoring them and the operational objective.

In the medium term, the initiative is expected to generate a strong positive impact with respect to the general objectives indicated under section 4.1.

Specific objective	Operational objectives	Indicators	Measurement tool
To reduce e-commerce VAT fraud by providing tax authorities with efficient and effective instruments for detecting non-compliant businesses	To give tax authorities access to relevant data to fight e-commerce VAT fraud	<ul style="list-style-type: none"> Number of audit carried out based on payment data Additional VAT collected by Member States 	<ul style="list-style-type: none"> Eurofisc annual report Eurofisc annual report
	To offer new or improved channels for EU Member States' tax authorities to share third party data	<ul style="list-style-type: none"> Central repository for payment data available for 99.9% of the time. Annual number of requests for information and spontaneous exchanges of information concerning the e-commerce sector between EU countries 	<ul style="list-style-type: none"> Commission report Annual statistics of the Member States
	To improve the identification and targeting of potential e-commerce VAT fraud	<ul style="list-style-type: none"> Number of fraudsters detected using payment data Number of requests for administrative assistance sent after detection of fraudsters through payment data 	<ul style="list-style-type: none"> Eurofisc annual report Annual statistics of the Member States

9.2. Monitoring structure

The Eurofisc reports and the annual statistics of the Member States are presented and discussed in the Standing Committee on Administrative Cooperation in accordance with Article 49 (EU) No 904/2010, which is chaired by the European Commission. The Commission will report the European Parliament and the Council on the application of the new system.

The evaluation of this initiative will take place after few years from the entry into force of the new system (taking into account at least few years to implement the new electronic databases). As such, the evaluation of the current initiative will be probably after the evaluation of the VAT e-commerce Directive. However, the evaluation of the current initiative will take into account the outcome of the VAT –e-commerce evaluation.

10. ANNEXES

10.1. Annex1: Procedural information

10.2. Annex2: Consultation synopsis report

10.3. Annex 3: Evaluation

10.4. Annex 4: Who is affected by the initiative and how

10.5. Annex 5: Methodology

10.6. Annex 6: Technical feasibility of the options

10.7. Annex 7: Case study – pricing policy and estimation of potential VAT loss

10.8. Annex 8: Result of the TAXUD 2016 survey on e-commerce compliance strategies in the EU

10.9. Annex 9: Payment Services' framework in the EU

10.10. Annex 10: B2B import VAT fraud

10.11. Annex 11: Third countries using payment data as VAT control tool

10.12. Annex 12: Visual examples of the regulatory options

10.13. Annex 13: Comparison amongst different initiatives in terms of fighting e-commerce VAT fraud

10.1. Annex 1: Procedural information

1. Lead DG, Decide Planning references

The initiative of adopting measures to fight e-commerce VAT fraud was in the VAT Action Plan¹⁴⁸

TAXUD is the lead DG for this initiative. The agenda planning reference is PLAN/2017/2023.

2. Organisation and timing

The first meeting of the Inter-Service Steering Group was on 26 January 2018 where the context, the draft combined evaluation/impact assessment roadmap, the consultation strategy, the draft timeline and the problem tree were presented. The following directorates and services were present: CNNECT, FISMA, GROW, JUST, SG, SJ. The comments of the different services have been taken into account.

The second meeting was on 15 February 2018 and the updated problem tree, the draft questionnaire for the public consultation and the options were presented. The following directorates and services were present: CNNECT, FISMA, GROW, JUST, SG, SJ. The comments of the different services have been taken into account.

The third meeting was on 23 March 2018 mainly to inform the different services and directorates on the state of play of the consultations and the tentative timeline. The following directorates and services were present: CNNECT, FISMA, JUST, SG.

The fourth meeting was on 5 April 2018 to present the draft of the first part of the Impact Assessment report. The following directorates and services were present: DIGIT, SG, SJ. The comments have been taken into account.

The Fifth meeting was on 24 May 2018 to present the second draft of the full Impact Assessment report. The following directorates and services were present: FISMA, SG, SJ, HOME, and DIGIT.

3. Consultation of the RSB

The Regulatory Scrutiny Board was consulted on 27 June 2018. The opinion of the Board was positive. The Board made a number of key recommendations to improve the report with respect to the following aspects:

- The description of the context is not sufficiently clear on the political support behind the initiative and the urgency to act;
- The baseline does not adequately project the potential impact of other recently adopted or proposed initiatives designed to combat VAT fraud. The differences between the options are not clearly described. As a result, the reasons for their distinct costs and impacts are not evident.

The report was adjusted to take into account the Board recommendations.

4. Evidence, sources and quality

¹⁴⁸ COM(2016) 148 final of 7.4.2016 Communication From The Commission To The European Parliament, The Council And The European Economic And Social Committee

The evidence for the impact assessment report was taken by different consultation activities:

- A 2016 survey with the Member States' tax authorities on e-commerce anti-fraud strategies
- The consultation with the VAT forum Commission Expert group on e-commerce
- The evaluation of Evaluation of Regulation (EU) 904/2010
- A targeted consultation addressed to tax authorities on payment data
- A targeted consultation addressed to payment service providers and businesses on payment data
- A public consultation
- Desk research

10.2. Annex 2: Consultation synopsis report

1. Consultation activities carried out

For the preparation of this initiative, the Commission launched a public consultation and a targeted consultation. The objectives of the consultations were to:

- collect data and evidence needed to evaluate the application of Regulation (EU) 904/2010 on administrative cooperation and combating fraud in the field of VAT in respect of VAT fraud on B2C cross-border supplies (hereinafter e-commerce VAT fraud);
- gather necessary knowledge in order to assess various options for the collection and exchange of VAT-relevant payment data as a tool for combating e-commerce VAT fraud;
- offer the public and stakeholders the opportunity to contribute meaningfully to the exercise and gather their views on the initiative at stake.

Further detailed regarding the public and targeted consultations are given below.

The Inter-Service Steering Group was consulted on the content of the Consultation Strategy and on the draft questionnaire for the public consultation.

1.1. Public consultation

The public consultation period was between 27 February 2018 and 25 April 2017 and was available in the 23 official EU languages. Based on TAXUD's request, the Secretariat General agreed with three derogations in order to limit the duration of the public consultation, the translation date into all EU languages and the shorter feedback period for the inception impact assessment. The derogations were due to be in line with the time line for the adoption of the initiative.

In order to increase the visibility of the public consultation, the Commission promoted this consultation on social networks: Twitter and LinkedIn.

1.2. Targeted consultation

1.2.1. Tax authorities

All 28 EU tax authorities have been consulted by means of a dedicated questionnaire.

The consultation period with tax authorities was between 9 March 2018 and 13 April 2018 but several answers were received after the deadline: also the late answers have been taken into account.

1.2.2. Payment providers and other businesses

Payment providers and other businesses, including internet platforms, have been consulted by means of a targeted questionnaire. The deadline for answering was the 13th of April 2018. However, most of the answers were received after this date: also the late answers have been taken into account. The dissemination of the questionnaire was largely done through the network of the members of the Sub-group on e-commerce of the VAT Forum but several targeted mails were also sent to representatives of banks, card schemes and postal services.

1.2.3. Small and medium-sized enterprises (SMEs)

TAXUD invited SMEs to provide their feedback on this initiative by disseminating the public consultation questionnaire *via* the Europe Enterprise Network. TAXUD also invited the European Association of Craft, Small and Medium-sized Enterprises (UEAPME)¹⁴⁹ and Business Europe to answer the targeted consultation questionnaire.

1.2.4. Other private sector stakeholders

The public consultation has been flagged out to the Belgian Bitcoin Association as well as to consumers' representatives, through the European Consumers Association (BEUC - *Bureau Européen des Unions de Consommateurs*), a network covering 31 European countries, including all EU Members States. However, they have not answered to the consultation.

1.2.6. Other international organizations

The European Payment Council, an international no profit association representing 76 payment service providers, is responsible for managing four payment schemes across the Single Euro Payments Area (SEPA). The EPC was interviewed, on March 2nd, 2018, in particular as regard the feasibility of the proposed policy options.

Aiming to learn from previous similar experiences, TAXUD also consulted the Secretariat of the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a body of the Council of Europe. However, no contribution was received.

2. Stakeholder participation

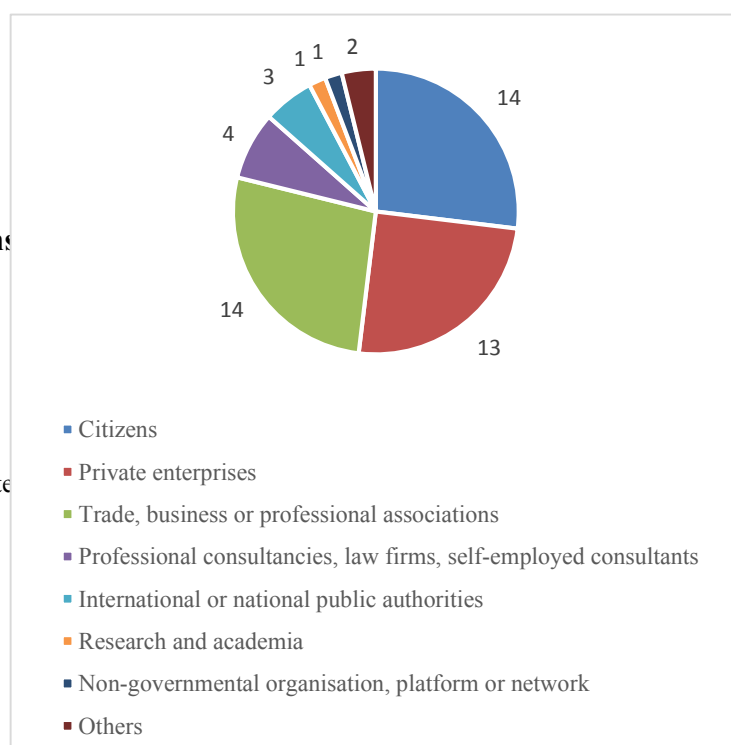
2.1. Categories of stakeholders

The identified stakeholders categories are composed of: (i) citizens, (ii) MSs tax authorities, (iii) businesses (payment providers, internet platforms, SMEs, other businesses), (iii) cryptocurrencies providers, (iv) consumers' representatives, (v) institutions and organizations with competences in the field of payment and anti-money laundering. The majority of stakeholders provided for feedback but at variable extent.

Figure 1: Respondents to the public consultation

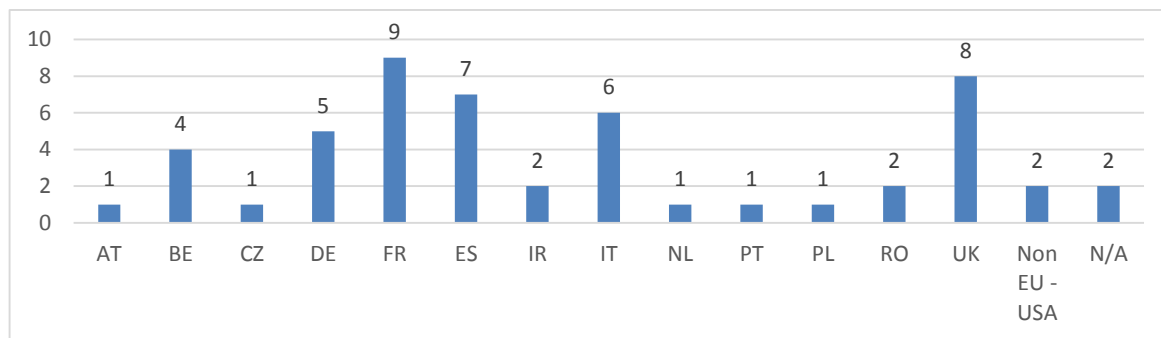
2.2. Participation in the public consultation

¹⁴⁹ UEAPME incorporates 67 member organizations federations, European branch federations and other associate



A total number of 52 answers were received by the end of the public consultation. Out of that, 14 respondents replied as citizens, in their personal capacity. The others (38 answers), responded in their professional capacity, as representatives of private enterprises (13), trade, business or professional associations (14), consultancies (4), international or national public authorities (3), research and academia (1) or other organisations (2).

Figure 6: Country of residence of the respondents to the public consultation (number)



The survey resulted in a relatively un-balanced representation in terms of number of respondents compared to the population of the respective Member States.

On the businesses side, only one respondent replying to the public consultation was a self-employed while five were large companies. The seven answers received from **SMEs** can be split as follows:

- 4 answers from businesses with fewer than 10 employees – Micro enterprises,
- 1 answer from businesses with 10 to 49 employees and
- 2 answer from businesses with 50 to 249 employees.

25 of the respondents replied in their professional capacity. Some of the respondents were representing associations active in the field of taxes or enterprises involved in e-commerce (sales of goods and services, including electronic gambling) which chosed to attach position papers or to make refference to other sites or content.

Furthermore, 20 replies to the public consultation originated from organizations registered in the Transparency Register.

Analising the public consultation replies, TAXUD did not detect a co-ordinated campaign for the submission of answers.

The majority of the respondents (up to 60%) seemed to represent businesses acting as traders (distance sellers) in e-commerce or associations and consultants representing their interests.

Even though more than half of the respondents demonstrated by their answers in the open questions a certain *expertise* regarding the e-commerce challenges and the tax administration’s practice, the information collected during the public consultation did not allowed for a clear conclusion on the *reputation, track record and longevity of the respondents*.

TAXUD processed the data and information collected through the public consultation, on the basis of an Excel spreadsheet, purely for the scope of assessing the possible impact of the current proposal, ensuring the appropriate protection of personal data without publishing the information of the respondents that did not give their consent.

2.3. Participation to the targeted consultation

From the **tax authorities'** side, TAXUD received 23 answers out of 28 possible despite the extended period for replies. Most of MSs' tax authorities faced difficulties in providing factual data on the size of the problem and the possible impact of the policy options. The reason of this lack of evidence is that the necessary data is held by third parties or authorities in other countries and Member States have no methodologies to make estimates in the field of e-commerce. In particular, the tax authorities rarely manage to monitor specific information on e-commerce because it refers to B2C transactions.

From the **businesses'** side, TAXUD received only 5 answers. One of the payment providers' association asked for an interview. The answers received from one of the banks demonstrate the good understanding of the challenges ahead and of the policy options and highlighted some of the issues related to the implementation of the initiative. However, this answer, despite acknowledging the problem and clearly indicating a preferred policy option, did not provide for sufficient data to assess the impact of the policy options on businesses. Finally, one of the large associations representing SMEs acknowledged the negative impact of the e-commerce VAT fraud on SMEs. However, that large SMEs association did not give any substantial contribution in respect of the policy options and possible impact on SMEs.

2.4. Consultation channels used

The Commission offered a set of diversified consultation channels:

- the public consultation questionnaire available via the EU Survey tool;
- two targeted consultation questionnaires, one for Member States tax authorities and one for businesses;
- an expert meeting of the Sub-group on e-commerce of the VAT Forum;
- an interview with the European Payment Council and a conference call with a payment services association;
- written contributions received directly by e-mail.

Despite the diversity of channels used, the number of contributions received remained small. The limited response rate to the public consultation can be explained by the rather technical aspects of the initiative at stake. However, the very limited number of answers of SMEs and payment providers in the targeted consultation was not expected.

3. Consultation results

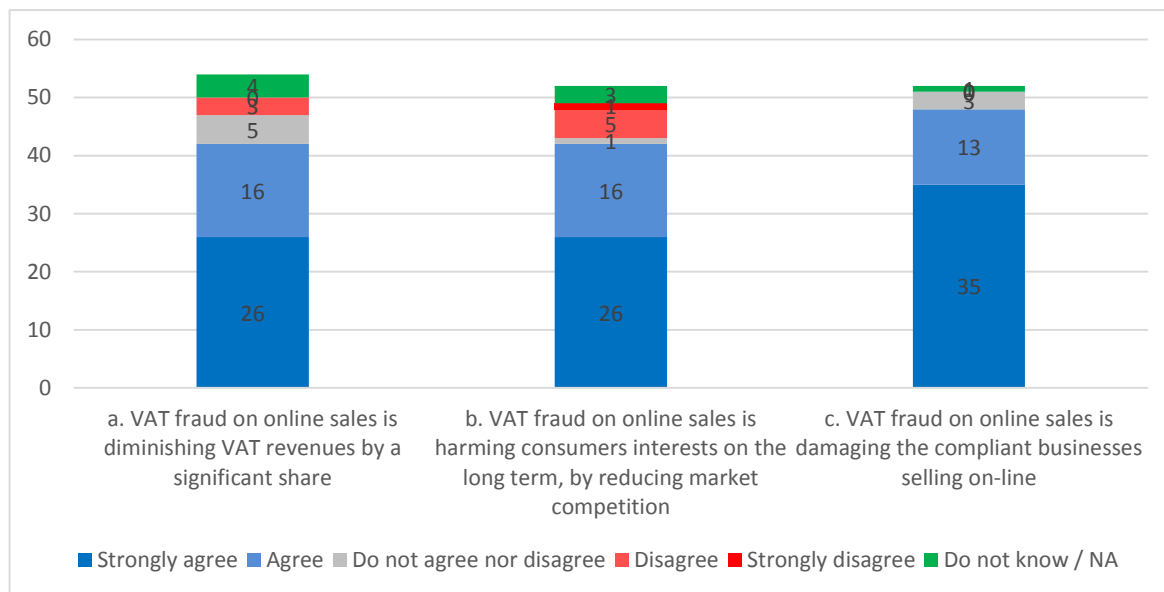
3.1. Results of the public consultation

Problem definition and size of the problem

The majority of those who answered the questionnaire perceived VAT fraud as an important problem. Most of the respondents (up to 48 out of 52) considered that the e-

commerce VAT fraud is damaging revenues, consumers and, finally, compliant businesses.

Figure 7: Perception of the negative impact of VAT fraud in e-commerce



The answers received confirmed that e-commerce VAT fraud might take various forms: (i) under-declaration of supplies and no VAT payment (40 opinions), (ii) non-registration of the remote supplier (39 opinions) and (iii) declaration and payment of VAT in a wrong Member State, to take advantage of a lower VAT rate (33 opinions).

Finally, from a quantitative perspective, most of the individuals and organisations answering the public consultation (35) were of the opinion that the e-commerce VAT fraud is a common problem in all the EU Member States. Several answers pointed to unfair competition from Asian suppliers of goods and at the breach of intellectual property rights associated with VAT fraud on the online computer games market.

Evaluation of the administrative cooperation

The majority of the respondents to the public consultation (28 answers) was unsatisfied with the **efficiency** of the fight against e-commerce VAT fraud (when comparing the results obtained and the resources invested). Only 10 respondents out of 52 considered the current fight against e-commerce VAT fraud efficient.

On the **effectiveness** of the current EU regulation, only 12 respondents replied that the EU Member States have the right tools to fight e-commerce VAT fraud while 32 respondents replied the opposite.

On the **EU added value**, the majority of respondents (27) seemed to agree that the existing administrative cooperation tools allow Member States to fight against e-commerce VAT fraud at a higher level than what could be achieved by the EU Member States acting independently.

From a **qualitative perspective**, most of the respondents considered that the causes of the lack of effectiveness in the fight against e-commerce VAT fraud are:

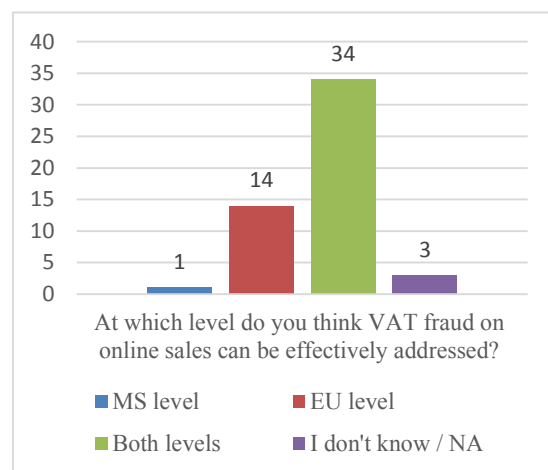
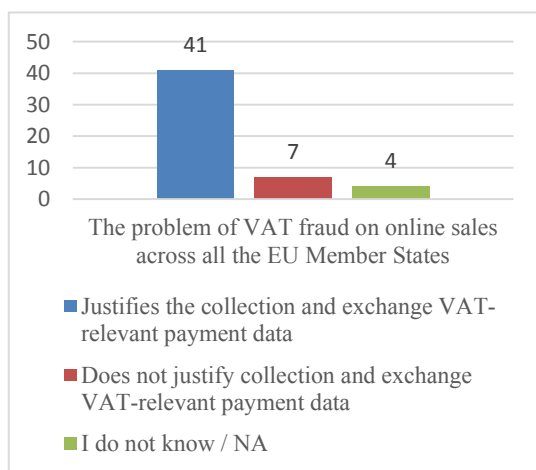
- lack of resources (people, money and even tools) for tax authorities compared to the volume of transactions to be verified;
- lack of willingness to cooperate between Member States' tax authorities;
- lack of cooperation between customs and tax authorities;
- absence of tools to enforce the VAT rules on remote suppliers from outside the EU and
- lack of cooperation from big platforms and marketplaces.

Subsidiarity and proportionality of the intervention

The majority of the respondents (34 out of 52) considered that **the e-commerce VAT fraud is a problem that should be addressed at both EU and Member States level** while an important number (14) of the respondents preferred the solution at **EU level** only.

As regard **proportionality**, the vast majority of the respondents (41 answers out of 52) considered that the collection and exchange of payment data is justified.

Figure 8: Proportionality of the initiative **Figure 9: Subsidiarity of the initiative**

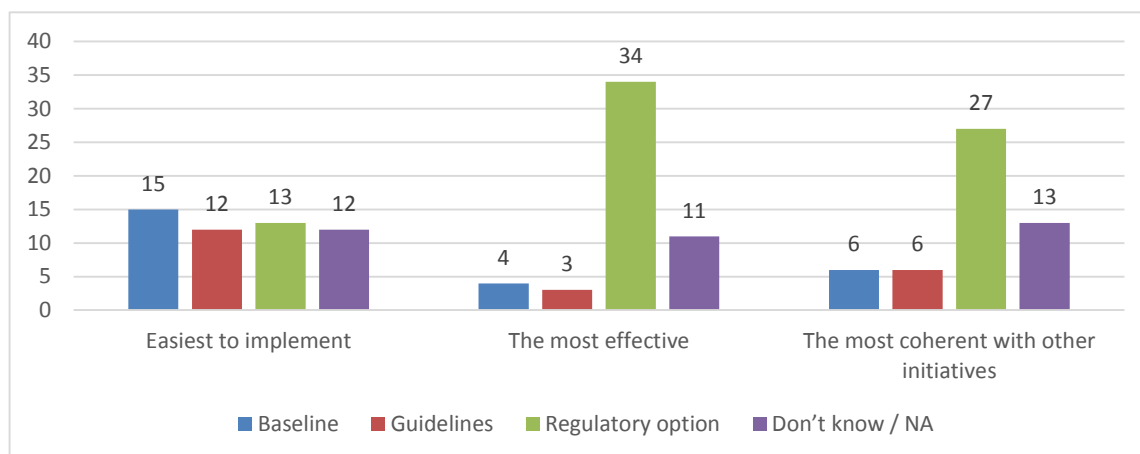


Policy options and their possible impact on all the stakeholders

In the questionnaire, the respondents were invited to express their view on the three main policy options and on different technical solutions.

The regulatory option, involving the collection and exchange of payment data, was the one preferred by the majority of respondents (fig. 6) because it was considered as the most effective for the fight against e-commerce VAT fraud.

Figure 10: Public consultation: Comparison of policy options



However, the analysis of the answers revealed that the preference for the regulatory policy option does not exclude the other options. Increasing the administrative capacity of Member States' tax authorities and issuing guidelines were perceived by the respondents as complementary or, at least, not excluding one another.

Most notably, in terms of efficiency, the option of investing only in the administrative capacity of the Member States' tax authorities was considered as easy to implement. This conclusion is consistent with some of the contributions received in relation to the open questions.

Within the regulatory option, the respondents expressed a preference for the central database (38 respondents) as means of collecting and exchanging payment data among tax authorities. However, respondents did not consider the choices as excluding one another. Therefore, some of the respondents also indicated a preference for the automatic exchange of information.

Figure 11: Public consultation: Preferred technical choices

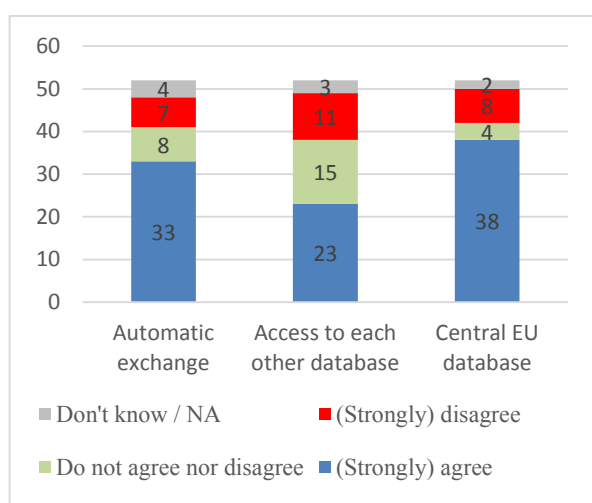
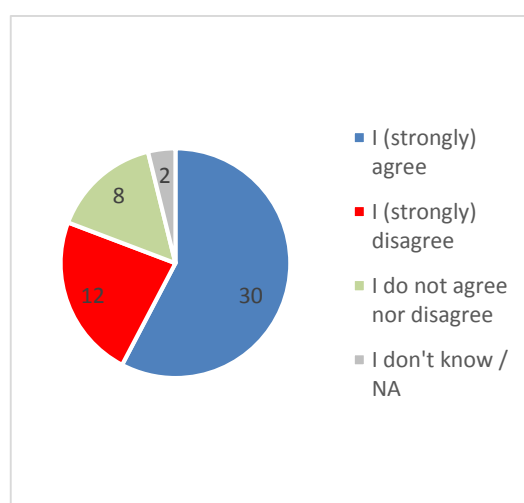


Figure 12: Public consultation: Exchange of data must not reveal the identity of the customer (buyer)



Protection of personal data

Concerning the protection of personal data, most of the respondents (30 out of 52) considered that the identity of the buyer should be protected and thus should not be exchanged between tax authorities. Only one respondent mentioned that the disclosure of this information may be necessary to assess VAT liabilities.

Overall, the majority of respondents mentioned that the collection of payment data is necessary (37 respondents) but, they pointed out the risks that data could be used for other purposes than detecting VAT fraud (35 respondents) and to identify the customer (35 respondents).

3.2. Results of the targeted consultation

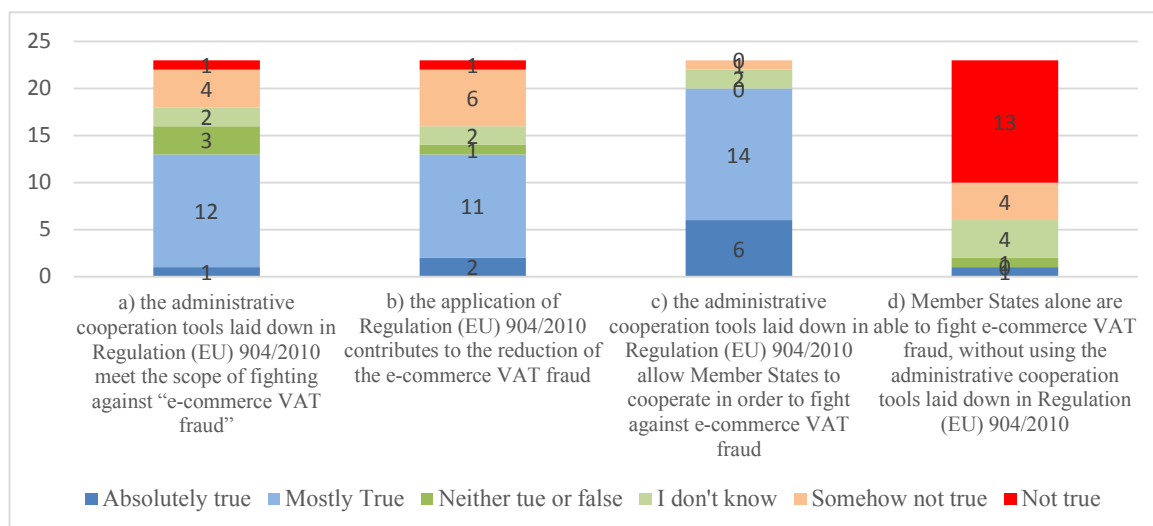
Despite the good response rate from tax authorities, there were few answers received from businesses. The Commission did not receive any feedback from consumers' associations, cryptocurrencies and anti-money laundering institutions.

Feedback from the tax authorities (answers received from 23 respondents)

Only three tax authorities were able to provide some partial **estimation of the VAT loss**. Furthermore, Member States were not able to estimate the loss of competitiveness of EU businesses due to e-commerce VAT fraud. However, more than half of the respondent tax authorities developed strategies to fight e-commerce VAT fraud. 14 tax authorities use internet-monitoring tools for detection purposes. Less than half of the tax authorities (12) already receive data from payment service providers at national level and 6 of the respondent Member States process third party data to detect e-commerce VAT fraud based on national risk analysis. Up to half of the responding tax authorities were able to indicate the number of tax audits on e-commerce during the last three years.

As regard the **evaluation of the current administrative cooperation tools** most of the responding tax authorities considered that they are still relevant but effective only to a limited extent. Member States mentioned difficulties in using administrative cooperation tools to fight e-commerce VAT fraud relating to: the identification of businesses over the internet; getting information from servers located outside the EU; insufficient level of resources allocated to fight e-commerce VAT; needs of more training for the staff; insufficient cooperation from some Member States, etc. Finally, nine tax authorities mentioned that other tools are needed in order to reinforce administrative cooperation. In particular, they indicated that tax authorities need access to third party data on e-commerce transactions, including data from payment service providers.

Figure 13: Tax authorities: evaluation of the administrative cooperation tools



Member States seemed to prefer the regulatory option. 18 respondents declared their tax authorities are in favour of an EU standard form to collect data from payment service providers while the only one opposing stressed that the central repository (payment providers uploading payment data directly to a central repository) is the only possible option to implement in a reasonable timeframe.

Regarding the **technical sub-options**, the majority of tax authorities (19 answers) supported the central repository, while only 10 of them found acceptable that payment service providers could transmit payment data only to one Member State of identification. Most of the respondents (18 answers) were in favour of a monthly reporting frequency for the transmission of payment data but against setting a threshold (14 answers).

With respect to **personal data protection**, almost half of the respondents (11 answers) mentioned difficulties when gathering and processing information collected from third parties. However, the difficulties seem mostly related to the reluctance of third parties to transfer data to tax authorities rather than to the lack of protection of the data once it has been handed over to tax authorities.

Feedback from businesses (answers received from 5 respondents)

E-commerce VAT fraud has a different impact on businesses depending on their field of activity. Payment service providers seem not to be affected by the problem or just indirectly affected to very little extent. The representatives of SMEs and other businesses indicated that e-commerce VAT fraud is widespread and that it is generating distortions and negative financial implications for honest businesses.

One association of payment service providers and two large **payment service providers** answered in the targeted consultation. The payment service providers confirmed they currently provide payment data to tax authorities, mostly on request. There is no clear indication of the costs incurred by these reporting obligations but one large payment provider mentioned that monthly transmission of information to national tax authorities generates work for one or two full time employees and yearly costs of around EUR 100.000.

The responding payment service providers confirmed that payment data is useful to fight e-commerce VAT fraud but also mentioned that some other sources of information may be needed (from internet platforms or marketplaces).

Payment service providers indicated there is a benefit in creating a single EU wide reporting standard for payment data instead of having various reporting obligations in different EU Member States. Some payment service providers expressed a preference for the regulatory option because it provides more legal certainty and effectiveness. One payment service provider indicated that the most cost-efficient solution is to transmit payment data to a central EU repository; another mentioned that data should be transmitted to the Member State of identification. The payment service providers expressed concerns of data protection if the payment data is transmitted directly from the payment service provider to a Member State different from the one of establishment.

The payment service providers considered the frequency of the reporting obligation as decisive for the costs of any reporting obligation (rather than reporting thresholds). A quarterly, semi-annually or annually submission of payment data seem to be reasonable by one of the associations representing payment service providers. Thresholds in reporting payment data may also be difficult to manage. In general, payment service providers were not able to quantify the administrative burden entailed in a new requirement on reporting payment data but only one of them considered that the collection of the data puts unacceptable additional burden on payment service providers.

From **other businesses**, different from payment service providers, TAXUD received only two answers in the targeted consultation: one from a very large SMEs association and another from an international association of VAT professionals and consultants. It is not clear if the policy options presented under this initiative have a direct impact on their members.

4. Conclusions

The results of the public and targeted consultations allowed the Commission to collect a significant number of views and opinions on the initiative. This **may not be representative at statistical level**, due to the relatively small number of answers (notably in respect to SMEs), but it is significant in terms of quality.

The quantity of data collected for evaluating the current administrative cooperation tools and assessing the possible policy options impact was very small.

All the data and views collected were used for the evaluation of the administrative cooperation tools in respect of e-commerce and for the impact assessment of the new initiative. The findings of the two consultations helped to assess the effectiveness, efficiency, relevance, coherence and EU added value of both the existing administrative cooperation tools as well as of the new policy options. The public consultation and the targeted consultation showed that the current administrative cooperation tools are still considered effective, efficient and relevant to a certain extent but also showed the vulnerabilities thereof. Moreover, the arguments collected through the consultations demonstrated the need to amend the current regulation on administrative cooperation, to allow for the exchange of payment data for fighting VAT fraud in e-commerce and to increase, in general, administrative capacity of tax authorities. All those arguments have been included and sometimes presented in more detail than in the current synopsis report, within the impact assessment report, i.e. chapters no.2 - *problem definition*, no.3 - *why should EU act*, no.6 - *impacts of the policy options*, and no.7 - *how do the options*

compare, as well as in the annexes no.3 –*Evaluation of Regulation (EU) 904/2010* and no.4 – *who is affected and how*. Finally, the feedback received through the public and the targeted consultations has been used to select the preferred policy option and assess the impact (mainly economic impact and on administrative and compliance costs). Hereunder are some of the key findings which have been used in the impact assessment report.

Both the public and targeted consultations **confirmed the problem definition** and the important size of the e-commerce VAT fraud. E-commerce VAT fraud has a strong impact on honest businesses by distorting competition. Some respondents gave examples to show the negative effects on several economic sectors heavily affected by cross-border non-compliant sellers. Tax authorities generally need to collect and exchange payment data in order to detect e-commerce VAT fraud and identify the VAT non-compliant suppliers. However, tax authorities may need access to other categories of data to crosscheck payment data for detection purposes.

Privacy was not mentioned as an important impediment to the collection and exchange of payment data as far as the personal data of the buyers (clients) receives a reasonable level of protection.

The majority of respondents expressed a preference for the regulatory option. In particular, the respondents indicated that the centralised repository is the most cost-efficient.

Tax authorities and payment providers **confirmed the added value of a EU wide standardised approach** for the collection and exchange of payment data but very few were able to estimate the positive impact in terms of supplementary VAT collection for any of the policy options.

10.3. Annex 3: Evaluation of Regulation (EU) 904/2010 for cross-border Business to Consumer online supplies

TABLE OF CONTENT

EXECUTIVE SUMMARY	66
1. INTRODUCTION	68
2. BACKGROUND TO THE INITIATIVE	68
3. EVALUATION QUESTIONS AND METHOD	71
3.1. EVALUATION QUESTIONS	71
3.2. EVALUATION MATERIALS	71
3.3. EVALUATION PROCESS AND MATRIX	72
3.4. LIMITATIONS AND ROBUSTNESS OF FINDINGS	77
4. ANALYSIS OF THE ANSWERS TO THE EVALUATION QUESTIONS	77
4.1. EFFECTIVENESS	77
4.2. EFFICIENCY	81
4.3. RELEVANCE	82
4.4. COHERENCE	85
4.5. EU ADDED VALUE	86
5. CONCLUSIONS	89

1. EXECUTIVE SUMMARY

The current evaluation is performed in conjunction with the impact assessment supporting the subsequent legislative proposal to amend Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value-added tax (hereinafter ‘Regulation (EU) 904/2010).

The objective of the evaluation is to examine to which extent Regulation (EU) 904/2010 met the overall objectives of contributing to a closer cooperation between Member States, of avoiding budget losses, of fighting VAT fraud and of preserving the principles of fair taxation, when considering e-commerce.

Although the stakeholders failed to provide the Commission with the expected level of factual data and the evaluation process has been marked by short deadlines, its findings

are strongly supported by the comprehensive evaluation of the Regulation (EU) 904/2010¹⁵⁰, finalised in 2017, and by the generally convergent views of numerous stakeholders. The Member States participation to the targeted consultation was significant (23 replies) and, thus, had a decisive contribution to building the conclusions of the current evaluation.

The general opinion concerning the administrative cooperation tools provided by Regulation (EU) 904/2010 and their application in relation to the e-commerce sector is favourable overall, even though it is more positive amongst the tax authorities than amongst the respondents to the public consultation. This situation is probably because tax authorities have a much better knowledge of the administrative cooperation process, which is mostly a back-office process, hardly visible for the public.

The administrative cooperation tools in the field of VAT seem to remain relevant, efficient and effective, even though the needs of the Member States to fight e-commerce VAT fraud are evolving. The effectiveness is partially hindered by the very specific information needs in the field of e-commerce VAT fraud: this information is often held in other countries and there are limited enforcement tools in respect of e-commerce VAT fraudsters located outside EU. In addition, some respondents pointed out the need to invest more in the administrative cooperation, by increasing the commitment of Member States and reducing the proportion of late replies on answering requests for information, but also by training the tax officials in the field of e-commerce. Finally, although factual data on the costs and benefits associated to the current administrative cooperation tools is scarce, tax authorities estimate that the benefits of employing the Regulation (EU) 904/2010 instruments are higher than or proportional to the costs. Several stakeholders raised the need to develop an automated system to exchange payment data as a valuable instrument permitting the detection of e-commerce VAT fraud. This last conclusion also resulted from the consultation carried out in the framework of the 2017 comprehensive evaluation.

The coherence of the current administrative cooperation tools with other EU policies and new initiatives has been confirmed. Most notably, as the Council adopted the e-commerce VAT Directive in December 2017, fully entering into force in 2021, Member States will heavily rely on administrative cooperation for checking on the correctness of VAT registration requests and of VAT returns. However, it was also noted that Member States should address new challenges such as the capacity of processing large volumes of data allowing for the detection of e-commerce VAT fraud. For the time being, except for some limited cases in which it was reported that banks or internet platforms denied access to data on grounds related to data protection rules, tax authorities did not face significant issues in complying with privacy regulations. For the future, the coherence of current administrative cooperation tools and data protection legislation may be challenged, as the e-commerce specificities require massive access to data and intense cooperation among tax authorities, both inside EU and with third countries.

Furthermore, the different stakeholders agreed on the EU added value of the administrative cooperation framework laid down in Regulation (EU) 904/2010. The administrative cooperation rules contribute to the protection of the Internal Market and of the VAT revenues. The e-commerce VAT fraud is affecting all EU Member States and,

¹⁵⁰ SWD(2017) 428 final, IMPACT ASSESSMENT accompanying the document *Amended proposal for a Council Regulation Amending Regulation (EU) No 904/2010 as regards measures to strengthen administrative cooperation in the field of value added tax*, Annex 3, p. 83.

due to the nature of e-commerce, Member States need to work together to detect fraud and enforce VAT rules. Stakeholders perceive that implementing individual Member States' remedies is rather ineffective and generally ask for more cooperation.

Overall, this evaluation shows that, despite a rather positive assessment of the current rules, new administrative cooperation instruments are needed to the Member States. Both the 2017 evaluation and the recent 2018-targeted consultation showed that Member States are generally in favour of exchanging payment data in order to cope with the shortcomings related to the effectiveness, relevance and coherence of the current rules of administrative cooperation. Therefore, exchanging payment data is one area in which Regulation (EU) 904/2010 may be further amended to give the tax authorities the right tools to cooperate in the fight against e-commerce VAT fraud.

2. INTRODUCTION

This proposal is a follow-up of the Commission's commitment to "address VAT fraud in the electronic commerce sector" by "working on proposals for third parties involved to supply targeted information to tax administrations in order to allow the latter to cope with the new e-commerce business models". It complements the recently adopted VAT e-commerce package that modernizes and simplifies the VAT system on B2C cross-border supplies of goods and services and the recent proposal amending the rules on administrative cooperation and combating VAT fraud adopted by the Commission in November 2017 (and mainly addressing B2B transactions). This initiative wants to provide tax administrations with appropriate tools to detect fraudsters and control VAT liabilities on cross-border Business-to-Consumer (B2C) supplies (hereinafter e-commerce) by collecting and sharing VAT relevant payment data. It should also ensure a level playing field for businesses and adequate data protection for any VAT-relevant payment data concerned.

A comprehensive evaluation of Regulation (EU) 904/2010 was carried out in 2017, covering the period from the entry into force of the Regulation until mid-2017. That assessment covered all the EU Member States, including Croatia.

Therefore, the current evaluation is not a fully-fledged evaluation of the administrative cooperation instruments laid down in Regulation 904/2010 but it is rather focussing on how the Regulation is applied in relation to the specific case of e-commerce VAT fraud, building on the general findings of a previous extensive evaluation.

In particular, this evaluation examines to which extent Regulation (EU) 904/2010 met the overall objectives of contributing to a closer cooperation between Member States, of avoiding budget losses, of fighting VAT fraud and of preserving the principles of fair taxation, when considering e-commerce.

The result of the evaluation is feeding into the proposal to amend the Regulation (EU) 904/2010 in order to give a substantial contribution to the fight against e-commerce VAT fraud. The aim is to learn about the administrative cooperation tools in use based on the application of the Regulation (EU) 904/2010 and to check whether changes or even new cooperation tools are needed.

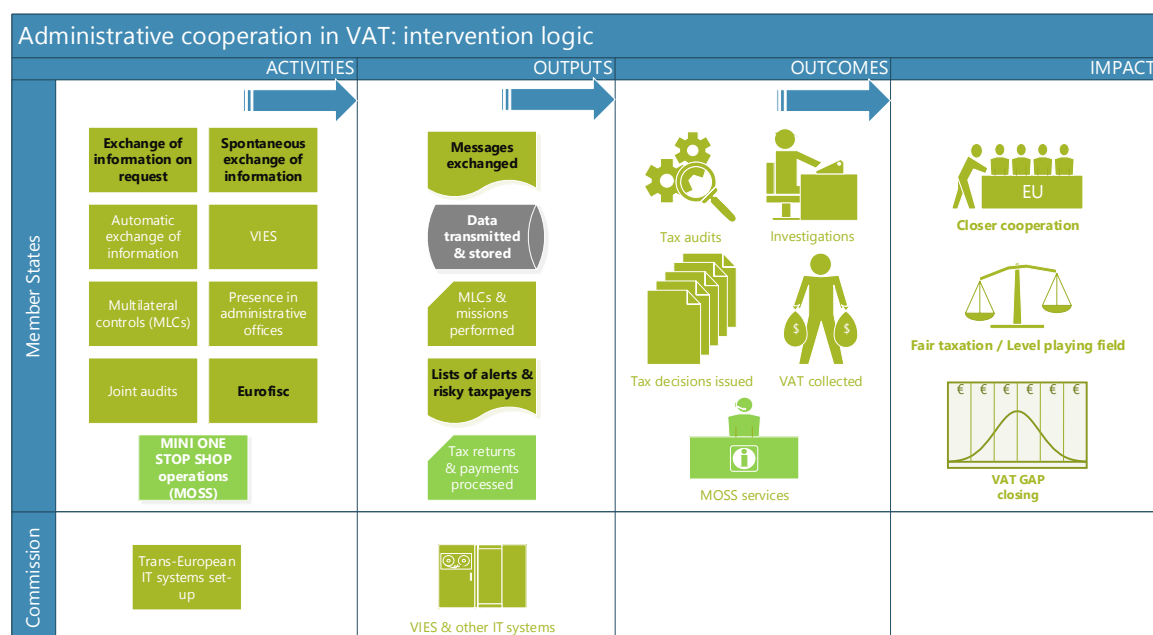
3. BACKGROUND TO THE INITIATIVE

Administrative cooperation in the field of VAT has been developing over time in order to better manage and control VAT in relation to the intra-EU B2B transactions and to ensure a level playing field for businesses.

Two main objectives were pursued with the introduction of Regulation (EU) 904/2010:

- to contribute to a closer cooperation between Member States; and
- to avoid budget losses, to fight VAT fraud and to preserve the principle of fair taxation.

Figure 14: Regulation (EU) 904/2010: intervention logic



Regulation (EU) 904/2010 currently in force lays down rule for the exchange of information between Member States tax authorities. The exchange of information can be on request, spontaneous (when a Member State informs another Member State of a possible breach of the VAT legislation in that Member State). A particular kind of spontaneous exchange of information is the automatic exchange (Member States periodically exchange a predefined set of data in specific fields). Furthermore, Member States' tax authorities can have automated access to each other databases on intra-EU B2B supplies (through an electronic system called VIES), carry out simultaneous controls and permit the presence of tax auditors from another Member State in administrative offices and during administrative enquiries. Finally, Regulation (EU) 904/2010 also set up a network for a multilateral exchange of early warning information to prevent VAT fraud, called Eurofisc.

All the above-mentioned tools, allow tax authorities to cooperate by collecting and exchanging sets of records and information originating from the businesses directly involved in the transaction chain. These sets of records and information are at the disposal of tax authorities or are easily accessible to them. However, in the cross-border

B2C online supplies, the relevant information may not be directly available to tax authorities¹⁵¹. Data about the transactions may, for example, be stored in another jurisdiction. Tax administrations often need access to data held by online platforms, payment service providers and other intermediaries, in order to identify any non-compliance. This presents legal and practical challenges depending on how and where data is held. Therefore, the "traditional" way tax administrations cooperate may need to be modernised.

The comprehensive evaluation carried out in 2017¹⁵² showed that Regulation (EU) 904/2010 suits the needs of the Member States and is coherent with other EU policies, existing or under implementation. The high level of cooperation demonstrates a good knowledge and application of this Regulation and shows its level of effectiveness and efficiency.

Overall, the Member States expressed a positive view regarding the legal and operational framework referring to Regulation (EU) No 904/2010. The vast majority considered that it helped improving administrative cooperation. Exchanges of information on request, automated access to information, Eurofisc and multilateral controls were considered as the Regulation's most effective instruments.

However, Member States should still work at national and EU levels to improve its functioning. For instance, that evaluation showed that new administrative cooperation instruments are needed by the Member States. The 2017 evaluation concluded that there is certainly room to further develop automatic and automated exchange of information. The categories of information that Member States considered as the most relevant were car registration information, data relevant for controlling e-commerce transactions and payment data held by financial institutions¹⁵³.

E-commerce was not considered as a separate area in the previous evaluation. Therefore, the current evaluation needs to assess whether the conclusions from the 2017 evaluation apply also to the VAT fraud in the field of e-commerce and indicate any provisions that may need to be revised or supplemented.

3.1. Application of the regulation

Regulation (EU) No 904/2010 only lays down the legal framework for tax authorities to cooperate for the fight of VAT fraud. The practical application of these tools is a responsibility of the Member States, and the success of the administrative cooperation depends on the way Member States' tax authorities commit and make use of the administrative cooperation tools.

Overall, the Member States expressed a positive view on the application of the tools provided by Regulation (EU) No 904/2010, in particular regarding the exchanges of information on request, automated access to information, Eurofisc and multilateral controls.

¹⁵¹ Because, under the VAT rules, the final consumer cannot offset the input VAT and, thus, does not have to keep any records of the purchase.

¹⁵² SWD(2017) 428 final and COM(2017) 706 final - Amended proposal for a COUNCIL REGULATION amending Regulation (EU) No904/2010 as regards measures to strengthen administrative cooperation in the field of value added tax, annex 3.

¹⁵³ SWD(2017) 428 final, p. 142.

However, over the last years, e-commerce volumes as well as cross-border sales increased at high rates. Despite the individual efforts of some of the Member States, VAT fraud in cross-border B2C e-commerce has become a true challenge.

In particular, according to a TAXUD survey launched in 2016 with tax authorities, only five Member States reported to have received spontaneous information on e-commerce VAT fraud from another tax authority under Regulation (EU) No. 904/2010. Furthermore, half of the respondent Member States to the survey reported difficulties in receiving information on request from other Member States on e-commerce VAT fraud.

The Commission launched in June 2017 an expert group called *e-commerce sub-group of the EU VAT forum*¹⁵⁴, composed of Member States' tax authorities and businesses representatives in order to provide for input in this area. The consultation showed that the main problem is in the lack of third party data (and in particular payment data) available to tax authorities and - thus - in the reduced chances of using administrative cooperation.

4. EVALUATION QUESTIONS AND METHOD

The evidence needed for the current evaluation made use of what collected through the comprehensive evaluation completed in 2017. In addition, TAXUD gathered evidence via a targeted consultation, a public consultation and desk research.

As the object of the evaluation remains Regulation (EU) 904/2010, the evaluation questions were mostly similar to those used in the comprehensive evaluation completed in 2017. However, the judgement criteria and the indicators are more specific, in order to focus on e-commerce.

4.1. Evaluation questions

The evaluation is based on the following questions (all of them focussing on e-commerce):

1. To what extent has Regulation (EU) 904/2010 contributed to a closer cooperation between Member States? (effectiveness)
2. To what extent has Regulation (EU) 904/2010 contributed to detect e-commerce VAT fraud ? (effectiveness)
3. To what extent has Regulation (EU) 904/2010 facilitated cooperation between Member States by making it smoother, faster and less burdensome? (efficiency)
4. To what extent the resources spent on the administrative cooperation generated results in the fight against e-commerce VAT fraud? (efficiency)
5. To what extent the provisions of Regulation (EU) 904/2010 continue to correspond to the needs of the Member States and other stakeholders in respect to e-commerce? (relevance)
6. To what extent are the provisions of Regulation (EU) 904/2010 in line with other policies and priorities of the EU in respect to e-commerce? (coherence)
7. Could Member States have achieved similar results without acting at EU level? (EU added value)

¹⁵⁴ Commission Decision 2012/C 198/05 of 3 July 2012 setting up the EU VAT Forum, OJ C198 of 6 July 2012; See: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012D0706%2802%29>

4.2. Evaluation materials

Views and evidence were collected by means of a questionnaire for a targeted consultation (addressed to tax authorities and businesses representatives participating in the Commission expert group "*e-commerce sub-group of the EU VAT forum*") and a questionnaire for a public consultation. The Commission services also had meetings with relevant experts and authorities and performed desk research.

4.2.1. Questionnaire to tax authorities¹⁵⁵

The questionnaire addressed to Member States' tax authorities aims at collecting views and evidence on all the evaluation criteria with a focus on e-commerce. On top of that, tax authorities were asked about the difficulties encountered in the application of Regulation (EU) 904/2010 and about the effectiveness of each of the administrative cooperation tools provided by the Regulation.

The tax authorities' consultation period was from 09/03/2018 to 13/04/2018 but was extended of additional two weeks.

4.2.2. Questionnaire to businesses¹⁵⁶

The questionnaire for businesses was made available through EU Survey and was addressed to payment providers and internet platforms. The aim of the questionnaire was, among others, to collect evidence and views from businesses on the compliance costs related to the fight against e-commerce VAT fraud. Some of the questions addressed the specific administrative burden in relation to the reporting requirements that businesses are must provide to tax administrations (notably payment data).

The businesses consultation period was between 12/03/2018 and 13/04/2018. However, most of the answers were received after the deadline.

4.2.3. Open-public consultation

The public consultation was designed with the purpose of collecting a maximum of evidence and views on the application of the evaluation criteria (relevance, effectiveness, efficiency, and EU added value). However, the public may have little knowledge of the administrative cooperation rules and mechanisms between competent authorities of the Member States. The public consultation was also made available through the SMEs portal.

The public consultation period was from 27/02/2018 to 25/04/2018.

4.2.4. Desk research

In order to collect evidence about the evaluation criteria, a number of papers, reports or other documents were consulted. Among those documents, the most relevant are:

1. SWD(2017) 428 final – the annex 3 – Evaluation of Regulation (EU) 904/2010 and
2. the answers form 21 Member States on the 2016 questionnaire concerning the administrative cooperation on VAT (AntiVATFraudEUMSE-commerce102016 – see 10.8).

¹⁵⁵ Ref. Ares(2018)1325223 - 09/03/2018 and follow up Ref. Ares(2018)1962904 - 12/04/2018

¹⁵⁶ Ref. Ares(2018)1354337 - 12/03/2018

4.3.Evaluation process and matrix

The evaluation process is based on analysing the compliance of the current administrative cooperation rules with the five criteria, according to the Better Regulation Guidelines, taking into account the specificities of the subject and the limitation described hereunder.

The planning of the evaluation has been integrated into the planning of the initiative on the collection and exchange of VAT-relevant payment data for e-commerce activities. The activities related to the component on evaluation, respectively to the component on impact assessment, are performed in conjunction, as a back-to-back exercise. The findings of the evaluation feed into the impact assessment, respecting the “evaluate first” principle.

The evaluation matrix presents the judgement criteria for each of the evaluation questions as well as the indicators used to assess the current situation and the data sources used.

Table 7: Evaluation matrix

Evaluation question	Judgement criteria	Indicators	Data source
1. To what extent has Regulation (EU) 904/2010 contributed to a closer cooperation between Member States? (effectiveness)	1.a. Development of the various forms of administrative cooperation between Member States on e-commerce VAT matters	1.a.1. Number of requests for information on e-commerce VAT fraud cases sent / received by EU MSs.	Questionnaire MSs 27 and 28 Evaluation 2017
	1.b. Difficulties in applying the tools of administrative cooperation in the e-commerce sector	1.b.1. Proportion of MSs reporting difficulties	Questionnaire MSs 29
2. To what extent has Regulation (EU) 904/2010 contributed to detect e-commerce VAT fraud? (effectiveness)	2.a. Positive stakeholder assessment of the administrative cooperation tools in relation to the detection and/or reduction of VAT fraud in e-commerce	2.a.1. Perceived effectiveness of the tools for administrative cooperation on e-commerce VAT fraud 2.a.2. VAT gap related to e-commerce	Questionnaire MSs 25a) Questionnaire MSs 25b) Questionnaire MSs 26 Questionnaire public consultation 33a), 33b)
	2.b. The tools provided by Regulation (EU) 904/2010 are considered adequate to fight VAT fraud	2.b.1. Perception of stakeholders on the adequacy of the means to fight e-commerce VAT fraud	Questionnaire public consultation 33a)
	2.c. The tools provided by Regulation (EU) 904/2010 are considered sufficient to fight VAT fraud	2.c.1. Proportion of stakeholders considering the tools as sufficient	Questionnaire public consultation 33b) Questionnaire MSs 31
3. To what extent the Regulation (EU) 904/2010 made the administrative cooperation between Member States smoother, faster and less burdensome? (efficiency)	3.a. Stakeholder's assessment of the administrative cooperation speed and burden in respect of e-commerce.	3.a.1. Perceived administrative burden associated with participation in administrative cooperation by Member States in respect to e-commerce	Evaluation 2017 Questionnaire MSs 31

Evaluation question	Judgement criteria	Indicators	Data source
4. To what extent the resources spent on the administrative cooperation generated results in the fight against e-commerce VAT fraud? (efficiency)	4.a. Benefits of administrative cooperation in the fight against e-commerce VAT fraud overweight costs	4.a.1. Reported ratio between costs and benefits resulting from the tools for administrative cooperation in respect of e-commerce	Questionnaire MSs 30
			Questionnaire public consultation 34
5. To what extent the provisions of Regulation (EU) 904/2010 continue to correspond to the needs of the Member States and other stakeholders in respect to e-commerce? (relevance)	5.a. The e-commerce VAT fraud problem determines the tax authorities to ask for administrative cooperation with other Member States	5.a.1. Number of requests for information on e-commerce VAT fraud cases generated by EU MSs.	Questionnaire MSs 27
			Questionnaire public consultation 36
	5.b. The size of the VAT fraud in e-commerce is significant	5.b.1. Number of Member States which have dedicated strategies / compliance programs 5.b.2 Cases of cross-border e-commerce VAT fraud 5.b.2. Number of Member States which reported supplementary tax liabilities following tax audits on e-commerce activities	Questionnaire MSs 10 Questionnaire MSs 4
6. To what extent are the provisions of Regulation (EU) 904/2010 in line with other policies and priorities of the EU in respect to e-commerce? (coherence)	6.a. Synergies with other EU initiatives	6.a.1. Qualitative assessment of the level of convergence of the objectives of Regulation 904/2010 with other Commission's strategies and policies	Questionnaire MSs 31 Desk research
	6.b. Identified areas that require to amend administrative cooperation rules in relation to e-commerce	6.b.1. Number of identified new tools/changes needed	Questionnaire MSs 31, 32

Evaluation question	Judgement criteria	Indicators	Data source
7. Could Member States have achieved similar results at similar costs without acting at EU level? (EU added value)	7.a. Joint EU approach in administrative cooperation in VAT has advantages over other forms of national and international forms of tax cooperation	7.a.1. Proportion of stakeholders having a positive perception of the advantages of a joint EU approach	Questionnaire MSs 25d) Questionnaire public consultation 33c)
	7.b. Stakeholders perceive the e-commerce VAT fraud as a common cross-border problem rather than as a national one.	7.b.1. Proportion of stakeholders considering the problem is not only national	Questionnaire public consultation 28g)
	7.c. The provisions of Regulation (EU) 904/2010 on cross-border administrative cooperation can be considered as providing EU solution to EU problems in terms of fighting e-commerce VAT fraud	7.c.1. Qualitative assessment of the tools that are appreciated by the MSs.	Questionnaire MSs 26 Questionnaire public consultation 36 Evaluation 2017

4.4.Limitations and robustness of findings

The evaluation of the existing administrative cooperation tools in relation to the e-commerce VAT fraud needs to rely at a large extent on the findings of the comprehensive 2017 evaluation of Regulation (EU) 904/2010. The current initiative mainly complemented and reconfirmed the 2017 findings by collecting data and views from a wide range of stakeholders. While the Member States participation to the targeted consultation was very positive (23 respondents) this was not the case for the other stakeholders, whom participation was very low. This could be explained by the technicality of the subject at stake.

There were essentially two types of limitations affecting this evaluation:

1. **Duration and resources.** The evaluation has been performed in the framework of a back-to-back exercise accompanying the new Commission initiative on collecting and exchanging payment data for fighting e-commerce VAT fraud. Because of the nature of the back-to-back exercise, the volume of work available had to be distributed between the evaluation and the impact assessment of the different policy options. Furthermore, the short timeline to perform the evaluation did not allow a study with an external consultant.
2. **Availability of data.** Data collected through the open public and the targeted consultation was limited. In particular the respondents did not provide precise data on:
 - a. e-commerce VAT gap estimations;
 - b. the number of cases of administrative cooperation in the field of e-commerce;
 - c. the costs of the administrative cooperation for Member States;
 - d. the supplementary VAT assessed as a result of the administrative cooperation activities.

For the purpose of this initiative, “e-commerce” refers to cross-border supplies of goods or services to final consumers. However, some of the tax authorities indicated that they do not have specific statistics because they miss a clear definition of "e-commerce". This is a possible explanation for part of the missing data, most notably in the targeted consultation.

However, even though quantification data are general missing, it was possible to collect many relevant qualitative opinions, including on the evaluation of the Regulation (EU) 904/2010 with respect to e-commerce VAT fraud. Unfortunately, the SMEs participation was quite low.

5. ANALYSIS OF THE ANSWERS TO THE EVALUATION QUESTIONS

5.1.Effectiveness

Q1. To what extent has Regulation (EU) 904/2010 contributed to a closer cooperation between Member States?

The Regulation (EU) 904/2010 entered into force in 2012. The exchange of information is significant, both in terms of volume and in terms of impact on cross-border VAT fraud. The exchange of information allows the tax authorities to detect un-reported or under-reported transactions in the e-commerce sector.

1.a. Development of the various forms of exchange of information between Member States on e-commerce VAT matters

According to the 2017 evaluation, the use of the various tools for exchange of information slightly increased: in particular, the total number of exchanges of information on request increased from 46.000 in 2012 to 49.000 in 2016. However, the decrease of the number of late replies seems to be more significant. Overall, the proportion of requests not answered within three months, decreased from 43 % in 2012 to 33 % in 2016. These trends are likely to apply also in the specific case of the administrative cooperation concerning the cross-border VAT fraud on e-commerce.

In the framework of the current back-to-back exercise, 23 out of 28 Member States answered the targeted consultation between March and April 2018. Based on the answers received, only 9 tax authorities confirmed that they have sent at least one request for information concerning e-commerce VAT fraud in 2017. Other 9 tax authorities were not able to provide any figure while 5 of them did not send any request on e-commerce in 2017. An overall number of 319 requests for information concerning e-commerce VAT fraud was sent in 2017. Almost half of this number originated from France only. It appears that, most of the Member States have no systems in place to monitor the number of exchange in the field of e-commerce. However, the number of exchanges in this field (319) is still very small when compared to the total number of requests for information processed annually by the Member States in the field of VAT (more than 45.000).

Member States received a total number of 124 requests for information referring to e-commerce VAT fraud in 2017. The highest number of requests (30) was received by Luxembourg.

Based on the 2016 survey concerning the administrative cooperation on VAT¹⁵⁷, 5 Member States indicated that under Regulation (EU) 904/2010 they received spontaneous information from another tax administration on e-commerce cases and 8 Member State received information on request. Unfortunately, the response rate for this question was quite low, with only 10 answers received.

Consultation with the Member States in the e-commerce sub-group of the VAT forum showed that VIES cannot be used systematically in the field of e-commerce because it only contains information on intra-EU B2B supplies. In 2017 the Member States set up a new Eurofisc working field dealing with e-commerce (WF5) but the exchange of information is still very limited (an indication of the number of exchange will be indicated in the next Eurofisc report which is - anyway - a confidential document only for the use of Member States tax authorities).

Finally, based on the data collected through the public consultation and the targeted consultation, it is not possible to conclude whether the use of the administrative cooperation tools to fight e-commerce VAT fraud increased since the entry into force of Regulation (EU) 904/2010. The limited information that the Commission was able to collect suggests a low level of cooperation on this specific matter.

1.b. Difficulties in applying the tools of administrative cooperation in the e-commerce sector

According to the 2017 evaluation, Member States have an overall positive opinion of the administrative cooperation framework laid down by Regulation (EU) 904/2010. In

¹⁵⁷ AntiVATFraudEUMSE-commerce102016

particular, the stable trend since 2013 in the number of requests for information, spontaneous and automatic exchanges shows a good appropriation of these tools by the Member States. Member States indicated that the most efficient tools are the automated access to information (VIES), Eurofisc and multilateral controls. However, Member States mentioned drawbacks, most notably in respect of the large number of late replies, the missing accuracy of data in VIES and the lack of commitment from some of the tax authorities.

The targeted consultation launched under the current initiative also revealed other shortcomings:

- (i) the identification of online businesses is difficult (do not have a physical address, do not always show a tax number);
- (ii) in the e-commerce, the domain of the online business is often located in another country and the relevant information about transactions is stored in non-EU countries;
- (iii) there are extremely limited enforcement tools in respect of non-compliant businesses selling online and which are located outside EU;
- (iv) tax officials need more training to be able to effectively use the administrative cooperation tools.

There is no indication of how frequently these difficulties occur. However, less than half of the respondent tax authorities (11) mentioned some difficulty in answering the requests for information on e-commerce cases while 12 respondents did not answer or did not indicate any difficulty.

Furthermore, several respondents in the public consultation were of the opinion that Member States do not have the resources and the tools for fighting e-commerce VAT fraud and do not cooperate enough. The public was also of the opinion that tax authorities face a heavy workload generated by the high number e-commerce transactions that require a huge effort in terms of investigations. This could result in a lack of interest in cooperating to fight e-commerce VAT fraud.

The consultation showed important difficulties in applying effectively the administrative cooperation tools in the field of e-commerce. This is partly due to the lack of access to relevant information and to the need of increasing the commitment of Member States to use administrative cooperation tools.

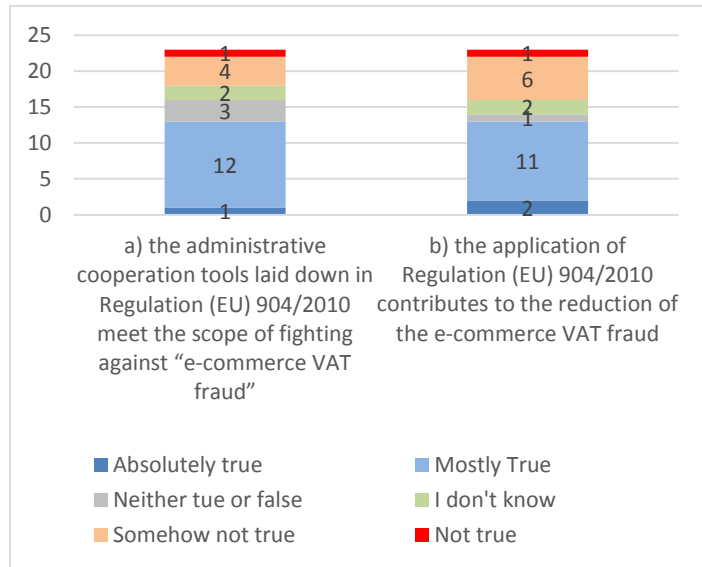
Q2. To what extent has Regulation (EU) 904/2010 contributed to detect e-commerce VAT fraud?

2.a. Perception of stakeholders on the effectiveness of the administrative cooperation tools in relation to the detection and/or reduction of e-commerce VAT fraud

The majority of the respondent tax authorities to the recent targeted consultation (13 out of

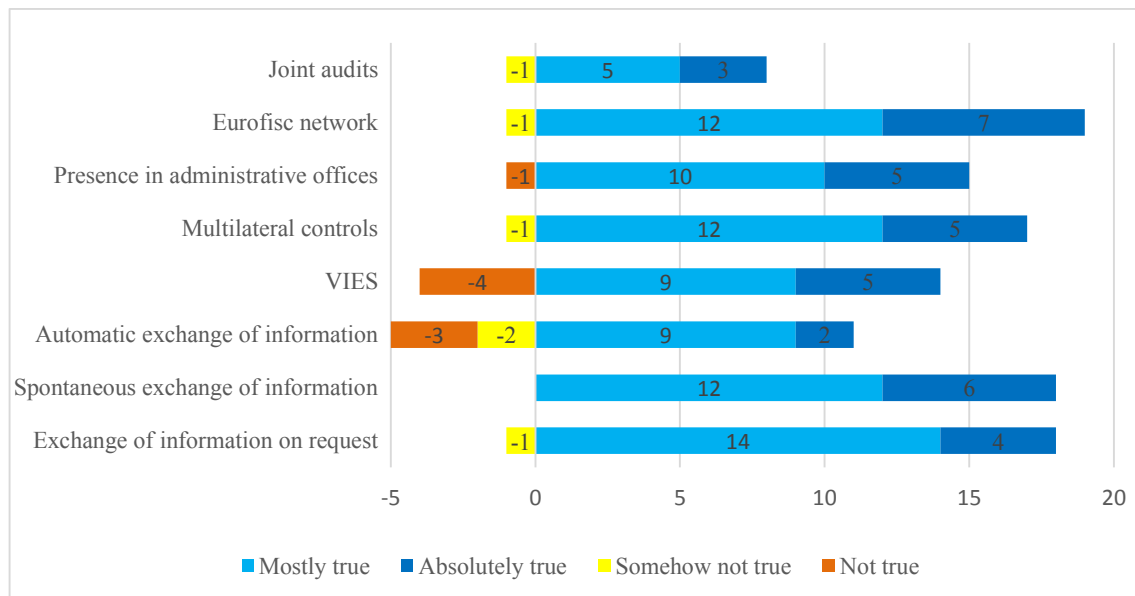
Figure 15: Tax authorities: perceived effectiveness of the administrative cooperation tools

23 answers) considered that the administrative cooperation tools laid down in Regulation (EU) 904/2010 meet the scope of fighting e-commerce VAT fraud and contribute to the reduction of the e-commerce VAT fraud. However, 7 respondents did not share this opinion, probably because they lack any quantitative evidence of e-commerce VAT fraud and of the impact of the administrative cooperation on it.



Member States showed similar opinions when questioned about the most effective tools for fighting e-commerce VAT fraud. The tools considered as most effective are: (1) the exchange of information on request - 18 positive opinions); (2) the spontaneous exchange of information - 18 positive opinions; (3) the multilateral controls - 17 positive opinions and (4) the Eurofisc network (19 positive opinions).

Figure 16: Positive and negative perception on the effectiveness of different administrative cooperation tools



Based on an external study, the Commission estimated that EU tax administrations are missing around EUR 5 billion of VAT revenue when consumers buy goods online from another country¹⁵⁸. There are no estimates of the VAT gap caused by cross-border online services. Presumably, in the absence of the administrative cooperation tools provided by Regulation (EU) 904/2010, the level of the VAT gap could have been larger but there is no evidence to demonstrate this.

¹⁵⁸ Commission SWD(2016)379 final, point 3 p. 13.

2.b. Perception of stakeholders on the adequacy of the means to fight e-commerce VAT fraud

In the 2018 public consultation, only 12 respondents indicated that the EU Member States have the adequate tools to fight e-commerce VAT fraud while 32 respondents indicated the opposite because the shortage of resources and "legal powers" and not enough cooperation between tax authorities for the fight against e-commerce VAT fraud.

2.c. Proportion of stakeholders considering the tools as sufficient

In the 2018-targeted consultation, the majority of tax authorities indicated that the current Regulation allows for a fair level of administrative cooperation, even though some of them recognised that there is a need of supplementary tools, including the exchange of payment data.

However, in the public consultation only 7 respondents replied to believe that the instruments at the disposal of the EU Member States are sufficient to fight e-commerce VAT fraud. This number even decreases to only 4 if we count only those respondents which declare having a good or partial familiarity with the subject. On the opposite side, 36 respondents believe that the tax authorities do not have sufficient instruments to fight VAT fraud on online sales.

As a preliminary conclusion, it appears that the effectiveness of Regulation (EU) 904/2010 in respect to e-commerce VAT fraud is limited compared to other types of fraud. Member States indicated that the effectiveness of the administrative cooperation tools are affected by different shortcomings such as problems to identify the online businesses, the volume of resources needed for an effective cooperation (staff and IT) and the lack of incentives to protect the tax base of other Members States (more spontaneous exchange of information is needed).

5.2. Efficiency

Q3. To what extent Regulation (EU) 904/2010 made the administrative cooperation between Member States smoother, faster and less burdensome?

3.a. Stakeholder's assessment of the administrative cooperation speed and burden in respect of e-commerce

The 2017 evaluation determined that most significant burdens are linked to human resources to deal with requests for administrative enquiries, reply to requests for feedback and participate in multilateral controls. However, those administrative cooperation tools seem to be very effective.

The 2017 evaluation indicates that, under Regulation (EU) 904/2010, the proportion of requests for information not answered within three months, decreased from 43 % in 2012 to 33 % in 2016. Despite this progress, there is still a considerable space for improving the speed of answering the requests for information from other Member States. In the case of e-commerce, the speed may be particularly affected by the low capacity of tax authorities to retrieve information on on-line sales, by the high volume of transactions and by the very labour intensive approach of the exchange of information based on case-by-case requests from other Member States.

As such, the logical solution would be to improve as much as possible the work productivity by investing in more resources in order to make a better use of these tools.

In 2018, 10 tax authorities reiterated problems due to late replies and limited cooperative approach from other Member States. This may lead, indirectly, to the conclusion that the framework laid down by Regulation (EU) 904/2010 does not imply difficulties for the use of administrative cooperation tools. The difficulties encountered by the tax authorities mostly result from objective external causes, as described above.

Finally, the targeted consultation did not lead to the collection of relevant statistical data concerning the ease of exchanging information. The number of cases in which Member States use administrative cooperation in respect of e-commerce VAT fraud remains low and mostly unreported. Therefore, it is not possible to draw a clear conclusion on the burden of the administrative cooperation activities.

Q.4. To what extent the resources spent on the administrative cooperation generated results in the fight against e-commerce VAT fraud?

4.a. Benefits of administrative cooperation in the fight against e-commerce VAT fraud overweight costs

The majority of the respondents to the public consultation (28 answers) was not satisfied with the efficiency of the fight against e-commerce VAT fraud (when comparing the results obtained and the resources invested). Only 10 respondents considered the fight against e-commerce VAT fraud as efficient.

The costs and benefits of the administrative cooperation tools in fighting e-commerce VAT fraud cannot be assessed based on factual evidence. Member States lack monitoring tools to measure the extent to which administrative cooperation has contributed to assess additional VAT. Little information referring to all type of VAT fraud (not specifically to e-commerce) may be drawn from the 2017 evaluation. That evaluation showed that Multilateral controls (MLC) led to an average result of EUR 18,5 million additional liabilities (VAT and direct taxes).

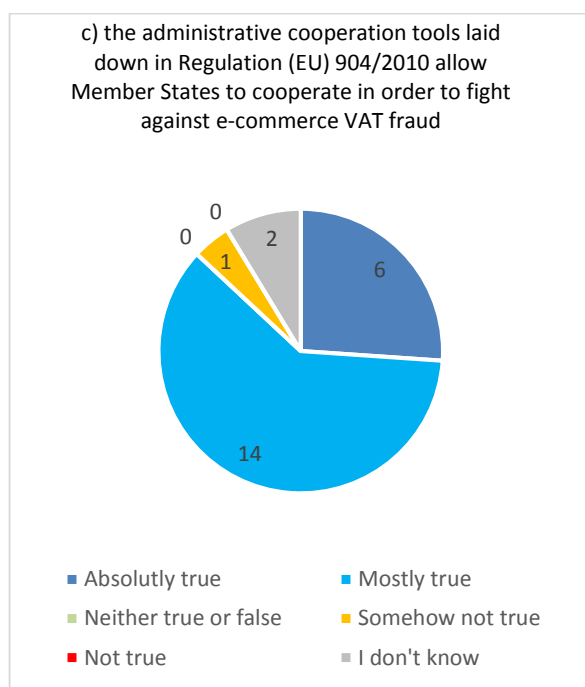
However, as per the comprehensive 2017 evaluation, 25 out of 27 Member States strongly agreed or agreed that costs associated with participating in administrative cooperation are proportionate to the benefits. The same perception results from the 2018 targeted consultation. Most of the tax authorities were not able to provide data or to estimate the level of resources involved. However, none of them was of the opinion that the resources involved in the administrative cooperation overcomes the benefits while 5 tax authorities considered that the administrative costs due to the use of administrative cooperation under Regulation (EU) 904/2010 to fight the “e-commerce VAT fraud”, are low or fair compared to the higher VAT revenues. The 2017 evaluation also concluded that the highest costs for tax authorities are associated with requests for information and administrative enquiries, multilateral controls and Eurofisc.

Therefore, despite the lack of factual data, tax authorities estimate that the benefits of administrative cooperation are higher than or proportional to the costs.

5.3.Relevance

Q5. To what extent the provisions of Regulation (EU) 904/2010 continue to correspond to the needs of the Member States and other stakeholders in respect to e-commerce?

Figure 17: Tax authorities: perception on the administrative cooperation tools



The relevance of the current Regulation (EU) 904/2010 in fighting e-commerce VAT fraud is assessed by checking the needs of the member States' tax authorities and on the effectiveness of the administrative cooperation tools.

The targeted consultation showed that Member States have adequate tools in the Regulation 904/2010/EU but there is room to use these tools more intensively and to develop new ones.

In addition, the 2017 evaluation showed that the Member States generally recognise that the administrative cooperation instruments are relevant. Requests for information, Eurofisc, MLCs and administrative enquiries score particularly high.

5.a. The cross-border VAT fraud problem in e-commerce determines the tax authorities to ask for administrative cooperation with other Member States

The 2018 consultation showed that tax authorities have sent only a small number of requests for information (319 cases). However, due to lack of statistical system of the Member States, this figure results from the information received from only 14 Member States.

Furthermore, Member States expressed support for administrative cooperation tools such as Eurofisc and MLCs. The majority of Member States recognised that more intense administrative cooperation is needed to fight e-commerce VAT fraud. The same conclusion is supported by the findings of the 2017 evaluation of the administrative cooperation as well as by the results of the 2016 Survey concerning the administrative cooperation on VAT.

Those Member States which developed VAT investigation and compliance strategies in the field of e-commerce are all facing an increasing need for data. In order to assess VAT liabilities, tax authorities must crosscheck the information referring to online businesses established abroad with VAT, MOSS and Customs information. When potential VAT fraud is detected, a request for administrative enquiry is sent to the State of establishment of the online business. In general, in order to detect e-commerce VAT fraudsters, tax authorities need access to information such as:

- business identification: name and address, tax identification number (and VAT number, if existing), IP numbers or other information needed to identify activities over the internet;
- information on transactions (flow of goods/services and flow of payment), including the description of the supply, the date, currency and value of the sales, bank account / payment methods, etc.;
- information on delivery channels (like, for example, the fulfilment centres and the carrier transporting the goods).

The consumers have no record keeping obligations. Therefore, all the relevant information is held either by the supplier in its country of establishment (different from the one of consumption) or by an intermediary such as payment service providers, internet platforms, or transport and logistic intermediaries, in cases of goods, which may be also established in another country. This explains why the tax authorities need to activate administrative cooperation in order to collect the necessary information to detect e-commerce VAT fraud and assess VAT liabilities.

Both from the side of the Member States requesting for assistance and the ones giving assistance under Regulation (EU) 904/2010, the two main difficulties refer to (i) the identification of the online businesses and (ii) the access to the relevant information that could be not accessible to tax auditors as it may be held in another jurisdiction or by third parties.

Finally, given the low number of requests for information concerning e-commerce, it is legitimate to wonder whether the administrative cooperation tools currently in force suit tax administrations needs in the field of e-commerce VAT fraud. Some of the Member States and part of the public suggested that, in order to detect e-commerce VAT fraud, exchange of massive volume of data, risk analysis and crosscheck processes must be put in place. Administrative cooperation granted on a case-by-case basis may not be relevant anymore when compared to the size and dynamics of the e-commerce, and its effectiveness in terms of VAT gap reduction is marginal. Even though Regulation (EU) 904/2010 allows automated access to data by electronic means, the specific tools, adapted to the exchange of massive VAT e-commerce relevant data, are still to be developed.

5.b. The size of the e-commerce VAT fraud is significant

As demonstrated by both the targeted and the public consultation, the size of the VAT fraud in the cross-border B2C e-commerce seems to be significant.

On the tax authorities' side, only three respondents provided for some partial estimation of the VAT loss but more than half of them developed strategies or plans to fight e-commerce VAT fraud. At least 14 tax authorities use internet-monitoring tools for detection purposes. Up to half of the responding tax authorities were able to indicate the number of tax audits on e-commerce in the last three years and the additional VAT assessed, per Member State, were ranging from modest amounts up to EUR 53 million.

The majority of the respondents to the public consultation perceived e-commerce VAT fraud as an important problem. Most of the respondents (48 out of 52) considered that the e-commerce VAT fraud is damaging revenues, consumers and, finally, compliant businesses.

The rapid global expansion of e-commerce is also a factor that may contribute to the size of the e-commerce VAT fraud, thus supporting the relevance of the administrative cooperation.

The 2018-targeted consultation showed that the majority of tax authorities consider that, generally, the current regulation allows for a fair level of administrative cooperation. On the other hand, 9 respondents among tax authorities indicated that other tools are needed to reinforce administrative cooperation, including access to third party data on e-commerce transactions. Considering the positive assessment of tax administrations regarding the effectiveness of the existing administrative cooperation tools, it is likely that Regulation (EU) 904/2010 is still relevant, at least for certain patterns of VAT the

fraud. The opinion of these tax authorities requiring additional tools, like the automated access to payment data, and the opinion of those answering the public consultation demonstrates that the rules of administrative cooperation need to be updated, to keep pace with the development of e-commerce and new business models in general.

5.4.Coherence

Q6. To what extent are the provisions of Regulation (EU) 904/2010 in line with other policies and priorities of the EU in respect to e-commerce?

The administrative cooperation in the field of VAT contributes to the proper functioning of the Internal Market. From this perspective, the administrative cooperation is crucial for supporting the free circulation of goods and services and for preventing any distortions arising from VAT fraud. Moreover, administrative cooperation supports contributes to the competitiveness of European businesses by ensuring a more level playing field. All these arguments prove that administrative cooperation is coherent with the objectives and general policies of the internal market.

6.a. Synergies with other EU initiatives

In December 2017, the Council adopted the e-commerce VAT Directive that will fully enter into force in 2021. The e-commerce VAT Directive abolishes distance sales thresholds, the VAT exemption on small consignments and introduces the One Stop Shop (OSS) to imports. The simplifications introduced with the e-commerce VAT Directive aim at improving VAT compliance by making the VAT system easier to comply with.

However, tax authorities still need the tools to detect and control the online businesses that will not comply with VAT rules even under the simplified regimes, or the ones that will declare less VAT than what actually due.

As seen the current Regulation (EU) 904/2010 allows tax authorities to exchange data on specific fraud cases, or to check VAT registration of businesses that have intra-EU supplies with other businesses (B2B). However, the current Regulation does not provide for specific tools to check the identity of cross-border B2C suppliers outside the MOSS or to automatically carry out any check on the real turnover of cross-border online businesses.

The extension of the MOSS and the introduction of the OSS on imports will represent an important opportunity for businesses, bringing substantive simplification for the fulfilment of VAT obligation on intra-EU supplies and imports. At the same time, it requires proper tools (such as collection and exchange of payment data) for tax authorities to check the reality and correctness of registration and tax declaration and, most of all, control the businesses outside the system to ensure a level playing field.

In fact, as mentioned before, the 2018-targeted consultation showed that 9 tax authorities asked for more administrative cooperation tools to fight e-commerce VAT fraud. The other tax authorities either do not have an opinion, or prefer to wait for the entry into force of the e-commerce VAT Directive in order to assess its relation with the functioning of the administrative cooperation under Regulation (EU) 904/2010.

These may lead to the conclusion that the current rules on administrative cooperation are largely in line with the other policies concerning the internal market and the recent e-commerce VAT Directive. Nonetheless, Member States should get prepared for new

challenges such as the capacity of processing data allowing for identification of e-commerce VAT fraud cases, which is difficult under the current regulatory framework.

6.b. Identified areas that require to amend administrative cooperation rules in relation to e-commerce

In the context of the targeted consultation the tax authorities did not precisely identified legal provisions in the Regulation (EU) 904/2010 which need to be improved. However - as already mentioned - they identified a few issues (in respect of the administrative practice) that require improvements:

- the high rate of late replies;
- the level of resources involved in administrative cooperation which is still too low, especially when compared to the volume of work imposed by the number of requests for information;
- the staff involved in the administrative cooperation needs more training;
- the Member States have to commit in granting a better assistance to other Member States.

In particular, some of the tax authorities mentioned¹⁵⁹ difficulties on accessing relevant data from internet platforms and payment providers (mainly because of data protection reasons).

Both the 2017 evaluation and the recent targeted consultation in 2018 showed that Member States are generally in favour of exchanging payment data and consider it as one area in which Regulation (EU) 904/2010 may be further amended to give the tax authorities the right tools to fight e-commerce VAT fraud.

5.5.EU added value

Q7. Could Member States have achieved similar results at similar costs without acting at EU level?

7.a. Joint EU approach on VAT administrative cooperation has advantages over other forms of national and international forms of VAT administrative cooperation

The EU can already rely and gain from a 40 years' experience of administrative cooperation between the Member States.

In order to control cross-border transactions, the Member States need to cooperate between each other because most of the time the VAT fraud is not restricted to their own territory. The tools foreseen by Regulation (EU) 904/2010 evolved during the time in order to respond to the need of Member States. These tools currently include exchange of information on request, spontaneous exchange of information, automatic exchange of information, automated access to data through VIES, multilateral controls, presence in administrative offices, presence during administrative enquiries, Eurofisc.

The respondents to both the open public and the targeted consultation stressed the advantages of common EU rules in order to allow Member States to work more closely together and fight e-commerce VAT fraud. In particular, the businesses claimed that a uniform approach as regard collection of VAT relevant data is more efficient and guarantees more legal certainty while tax authorities considered administrative cooperation as effective to combat e-commerce VAT fraud.

¹⁵⁹ As a result of the 2016 survey (AntiVATFraudEUMSE-commerce102016), at least in 7 cases, tax authorities mentioned difficulties of cooperation with internet platforms and even banks.

Figure 18 - Public consultation: Public perception of the EU added value

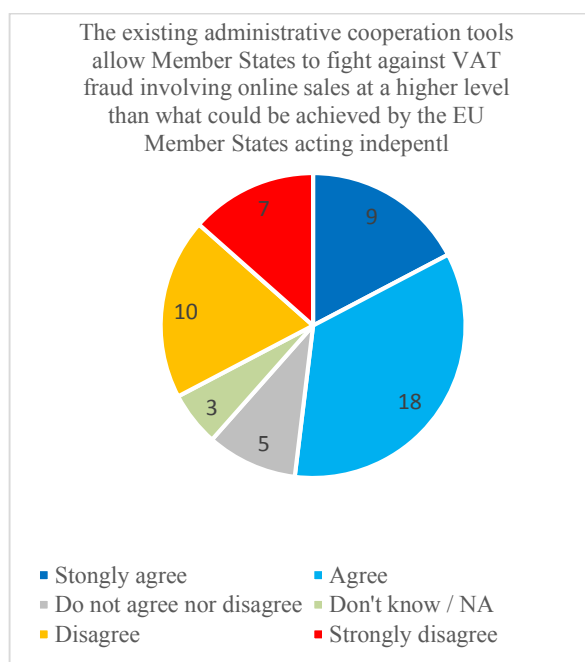
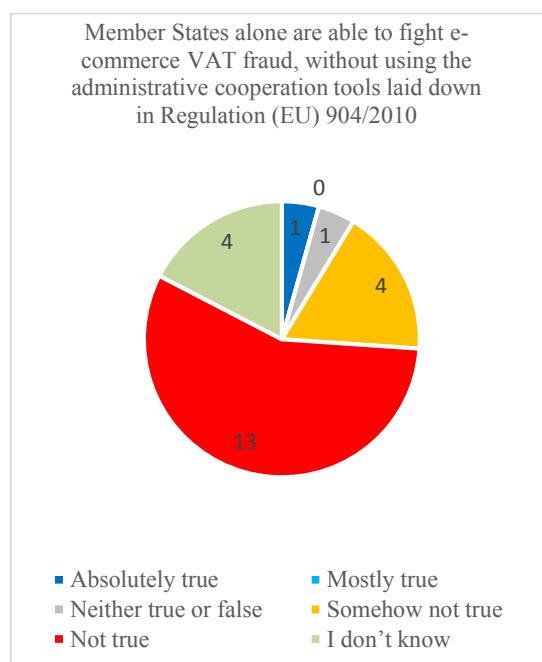


Figure 19: Tax authorities: perception of the EU added value



The perception of the majority of respondents to the public consultation (27 answers) was that the existing administrative cooperation tools allow Member States to fight against e-commerce VAT fraud more effectively than what could be achieved by the EU Member States acting independently. Furthermore, the majority of tax authorities answering to the 2018 targeted consultation (17 answers) agreed or strongly agreed that Member States alone would not be able to fight e-commerce VAT fraud need the tools of the administrative cooperation.

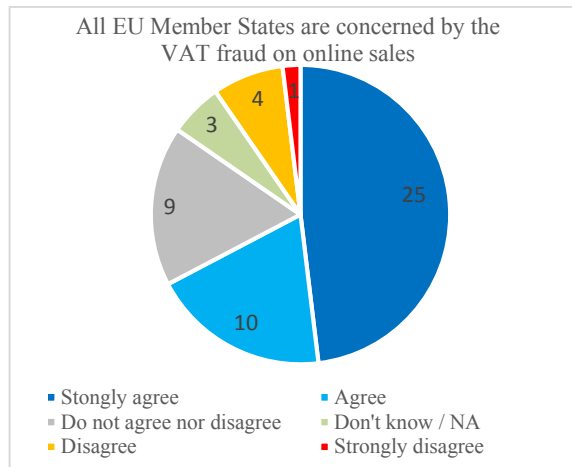
From another perspective, replacing the common EU framework of administrative cooperation in the field of VAT with other forms of national and international tax cooperation seems to be less effective and, possibly, more expensive. Currently, there is no other organization offering the same level of administrative cooperation in the field of VAT as the EU. OECD, for example, dedicates most of its recent efforts to the field of direct taxation while the level of mutual assistance for VAT which has been developed under the Regulation (EU) 904/2010 is unmatched by any other multi-lateral legal instrument in the field of taxation. Finally, the Fiscalis evaluations show, generally, that the trans-European IT systems in the field of taxation, like VIES, offer good value for money, as it would be more expensive for the Member States to develop independently national IT systems with an equivalent effect.

Finally, in 2017, 33% of the customers buying on-line across Europe shopped from sellers in other EU countries while 23% shopped from sellers outside EU¹⁶⁰. Therefore, one of the highest benefits of the administrative cooperation tools implemented based on Regulation (EU) 904/2010 seems to be the protection of the Internal Market.

¹⁶⁰ http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#e-shopping_from_other_EU_countries.

7.b. Stakeholders perceive the e-commerce VAT fraud as a common cross-border problem rather than as a national one.

Figure 20: Public consultation: perception on the e-commerce VAT fraud problem



There is no doubt that, by its nature and as explained above, e-commerce requires cooperation between tax authorities in order to assess VAT correctly. The destination principle makes this necessary, as the VAT is due in the country of consumption, even though the supply originates from another Member State or from a third country or territory. In order to protect the free circulation of goods and services within the Internal Market, tax authorities have to find ways of working together for protecting VAT revenues and for ensuring a level playing field for businesses.

The Customs Union require also to set common rules related to imports, thus when it comes to e-commerce VAT fraud, Member States have to find common EU solutions by using the administrative cooperation tools provided by Regulation (EU) 904/2010.

As highlighted by the public consultation, most stakeholders are aware of this “EU dimension” of the e-commerce VAT fraud. In fact, 35 respondents declared they consider that the e-commerce VAT fraud is affecting all EU member States.

7.c. The provisions of Regulation (EU) 904/2010 on cross-border administrative cooperation can be considered as providing EU solution to EU problems in terms of fighting e-commerce VAT fraud

The effectiveness of the tools for administrative cooperation gives an indication of their EU added value.

The results of the 2017 evaluation indicated that the most efficient tools provided by Regulation (EU) 904/2010 are the automated access to information (VIES), Eurofisc and multilateral controls.

In 2018 with respect to e-commerce, the tax authorities indicated that the most efficient tools are Eurofisc, followed by the exchange of information on request, the spontaneous exchange of information and the multilateral controls.

However, as highlighted by some of the tax authorities in the targeted consultation, the potential of the current administrative cooperation tools is not exploited at its best. The EU added value could be higher by increasing the use of the tools provided by Regulation (EU) 904/2010.

In essence, while the EU provides for the legal framework for administrative cooperation to combat e-commerce VAT fraud, its impact on VAT fraud depends on the resources invested and the commitments of each Member State to cooperate to reduce VAT loss at EU level and contributing to a level playing field for businesses in the Internal Market. This statement is also supported by the findings of the public consultation. In fact the majority of the respondents (34 out of 52) considered that the e-commerce VAT fraud should be addressed both at EU and Member States level while an important number (14)

of the respondents considered that the problem can be only solved at EU level. Only one respondent argued that e-commerce VAT fraud should be addressed only at Member States level.

In conclusion, the EU added value of administrative cooperation is the protection of the Internal Market and of the VAT revenues. E-commerce VAT fraud is a common problem, affecting all the Member States. Member States alone are not able to tackle the problem of e-commerce VAT fraud. Therefore, Member States should invest in administrative cooperation. Some of the administrative cooperation tools, like Eurofisc, seem to be rather well fitted for this purpose. However, the EU added value of the administrative cooperation is still somehow limited, as the level of resources invested in the administrative cooperation is not sufficient compared to the needs. New and more effective tools may still be needed.

6. CONCLUSIONS

The current evaluation assesses to what extent Regulation (EU) 904/2010 met the overall objectives of contributing to a closer cooperation between Member States, of avoiding budget losses, of fighting VAT fraud and of preserving the principles of fair taxation, when considering e-commerce. It mostly confirmed that the findings of the 2017 comprehensive evaluation of Regulation (EU) 904/2010 also apply to the specific case of e-commerce. The exception is that, in the field of e-commerce, the tax authorities consider the Eurofisc network and the exchange of information on request and spontaneous as the most effective tools, while the 2017 evaluation showed that VIES is the most appreciated tool. Indeed, VIES is conceived as a tool for sharing information on B2B intra-EU supplies and not on B2C transactions. For this reason, VIES does not fit with the need of fighting e-commerce VAT fraud.

With respect to the **effectiveness** of the current tools for administrative cooperation in relation to e-commerce VAT fraud, tax authorities have a better opinion than the public, probably because they have a direct knowledge of their application. In general, tax authorities consider the current Regulation (EU) 904/2010 on administrative cooperation as effective. However, there are a number of shortcomings:

- (i) the identification of online businesses is difficult;
- (ii) the domain and records of the online business is often located in another country (also outside the EU);
- (iii) there are limited enforcement tools in respect to VAT fraudsters located outside EU;
- (iv) tax officials need more training to use more effectively the administrative cooperation tools.

The needs to increase the commitment of Member States and dedicating more resources to administrative cooperation appear as crucial because they currently limit the effectiveness of the Regulation in respect of fighting e-commerce VAT fraud. Furthermore, some Member States also mentioned that the effectiveness of the Regulation could be increased with new tools, such as access and exchange of relevant payment data.

There is not sufficient quantitative evidence to support the **efficiency** of the administrative cooperation in respect of e-commerce. However, the opinions of the tax authorities are converging and positive, considering that the benefits of the administrative cooperation are proportional or even higher than the costs. This positive opinion is

consistent with the findings of the 2017 comprehensive evaluation. The evaluation also showed a need to increase the use of automated access to information.

The targeted consultation showed that the tools laid down in Regulation (EU) 904/2010 are **relevant** to fight VAT fraud but there is room for improvement. The evolution and the volume of e-commerce transactions may require new and more effective and efficient administrative cooperation tools. Therefore, the existing tools may become less relevant in the future due to the evolution of the business models and of the patterns of VAT fraud.

The analysis of the **coherence** of Regulation (EU) 904/2010 with other policies and priorities of the EU in the e-commerce sector showed a good level of alignment. In this respect, it is important to stress that administrative cooperation in the field of VAT contributes to the proper functioning of the Internal Market and, in particular, of the e-commerce VAT Directive rules. Nonetheless, Member States should deal with new challenges such as the capacity of processing data for the detection and fight against e-commerce VAT fraud.

Finally, the **EU added value** of the current tools of administrative cooperation, as provided by Regulation (EU) 904/2010, appears evident. Both tax authorities and other stakeholders recognised the benefits of acting together at EU level, as the e-commerce VAT fraud is affecting all EU Member States. Individual national measures are not considered effective enough.

Overall, both the 2017 comprehensive evaluation and the targeted consultation under the current initiative showed that Member States are generally in favour of collecting and exchanging payment data and amending Regulation (EU) 904/2010 accordingly. The findings of this evaluation must feed the legislative proposal to collect and exchange VAT relevant payment data to combat e-commerce VAT fraud.

10.4. Annex 4: Who is affected by the initiative and how?

The preferred option (sub-option 3.2) will imply **payment service providers** to keep records to be transmitted every quarter to the tax administration of establishment. The record keeping and the format of the transmission of data to tax authorities will be harmonised EU wide. Compared to the baseline scenario, payment service providers will benefit from common EU harmonised rules instead of dealing with different procedures in the Member States, thus leading to increased legal certainty.

Tax authorities will have to upload the data received in a centralised database, and manage the analysis of the data at Eurofisc level. The result of the risk analysis will have to be used by the Eurofisc officials to activate VAT controls. Compared to the baseline scenario, tax authorities will exchange payment data and will have to activate controls on the information received. There will be a level of direct costs for tax authorities which have been extrapolated from the costs of the Customs Information System (ICS2), which is another centralised database with a number of functionalities that could be similar to the ones foreseen in the preferred option. Besides the initial cost of developing the IT capabilities to collect massive volume of payment data, tax authorities will have to maintain their own systems. However, it is reasonable to expect that most tax authorities already have large scale capabilities of processing large volumes of data as most of them invested in the automatic exchange of information on direct taxes. With very few exceptions, tax authorities were not able to estimate the costs of implementing different policy options. Nonetheless, most respondents in the targeted consultation (16 answers out of 23) declared they are probably or certainly capable of storing the data received from the payment service providers established in their Member State in an electronic database.

Concerning the indirect costs, one could expect that tax authorities would have to dedicate limited resources to cross check the correctness of the payment data format or to log the information in the central repository. In fact, the payment data will be transmitted in an EU harmonised electronic format.

The **European Commission** will have to develop and maintain the central repository, but will not have access to transaction level information. However, the Commission should be allowed to extract statistical data for ensuring the security of the central repository and to follow up the performance of the initiative.

European citizens will not be affected when buying products. Their personal identification data will not be transmitted to the tax authorities. Data collected will refer to payees receiving payments from another state only. Moreover, only when risk filters will indicate that these payments could refer to an economic activity, the tax authorities will first carry out a preliminary crosscheck with other sources of tax information and eventually decide on a tax audit. Finally, the European citizens will be positively impacted by the higher VAT revenues resulting from the fight against VAT fraud and, probably, by a less distorted market.

European businesses and SMEs will benefit from the more level playing field resulting from the fight against VAT fraudsters. European businesses selling on-line will not be affected by any new reporting obligation.

In respect to costs for businesses, these are likely to have a limited one-off impact on payment providers. The limited impact is foreseen due to the automation of the business processes and to the fact that most payment providers seem to own already a strong IT support, allowing them to exchange large volumes of data with tax authorities or other entities (i.e. with members of the same economic group, other payment providers and clearance institutions, analytics companies, other providers of services on their behalf, etc.). At present, for example, one large payment providers mentioned costs of around 100.000 Euros / year for answering the case-by-case information requests from tax authorities (mostly generated by the time consumed by employees).

On the longer term, the costs for payment providers may result from the requirement of storing the information on a 10 years term and, more importantly, from the periodical effort to gather and transmit data. However, as reported by some payment providers during the targeted consultation, this requirement seems to exist already for some EU countries, even though for shorter periods. Equally, the prices for large storage capacities have been continuously decreasing over the recent decades, so this may not seem an unbearable cost. Finally, it remains only to mention that the reporting period seems to play a more significant role in respect to recurrent costs for payment providers. As suggested during the targeted consultation by one of the associations representing payment providers, quarterly, semi-annually or annually submission of payment data seem to be reasonable in terms of costs, thus leading back to the conclusion that the overall costs for payment providers will be limited.

Summary of costs and benefits

<i>I. Overview of Benefits (total for all provisions) – Preferred Option</i>		
<i>Description</i>	<i>Amount</i>	<i>Comments</i>
Direct benefits		
VAT collection increase		The investment costs of the tax authorities will be radically outweighed by the VAT revenue increase due to the fight against VAT fraud. An initial investment of EUR 180.000 in Finland (where such a system already exists at national level) led to a collection of more than EUR 16 million of VAT collected after targeted controls. As a result of the VAT collection increase, it is expected that the VAT gap will be reduced in the e-commerce sector.
Increased legal certainty for payment providers		Payment service providers will deal with the Member States' tax authorities through harmonised procedures and common reporting standards. This may first lead to a better predictability and less errors. Secondly, this may subsequently lead to some limited costs savings as payment providers will implement standardised IT systems and procedures for reporting in different EU countries.
Indirect benefits		
Level playing field		European businesses , including SMEs , both in the e-commerce and traditional economy, will benefit from the fight against VAT fraud. The number of fraudsters that benefit from unfair competition (thanks to the VAT fraud) is supposed to decrease, thus leading to a more level playing field.
Spill over effect on consumers		Businesses involved in e-commerce VAT fraud usually pay little attention to ensuring a good level of customer support, ensuring the legal guarantee for the products they sell and respecting intellectual property rights. This assumption has been confirmed by some answers in the public consultation. Even though the eviction of fraudsters from the market does not necessarily trigger a positive effect on those issues, there is a reasonable expectation that a number of customers will not be any more victims of poor customer services or the non-respect of intellectual property.

<i>II. Overview of costs – Preferred option</i>							
		Payment service providers		Tax administrations		European Commission	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Transmission payment data	Direct costs	limited	limited				
	Indirect costs		limited				
Storage and exchange of payment data	Direct costs		limited	EUR 7.5 million	EUR 2.9 million (1 year)	EUR 11.8 million	EUR 4.5Million (1 year)
	Indirect costs				limited enforcement costs		

10.5. Annex 5: Methodology

It was not possible to carry out a quantification of the impacts of this initiative through a CGE (computable general equilibrium) model simulation in the time available. The analysis of the impacts will therefore be laid out essentially in qualitative terms.

The evidence for the impact assessment report was taken by different consultation activities:

- A survey with the Member States' tax authorities on e-commerce anti-fraud strategies
- Consultation with the VAT forum Commission Expert group on e-commerce
- A targeted consultation addressed to tax authorities on payment data
- A targeted consultation addressed to payment service providers and businesses on payment data
- A public consultation
- Desk research

Furthermore, a feasibility study has been carried out internally in TAXUD calculating the costs of the different options. For the quantification, the study (Annex 6) considered the costs of the Import Control System, which presents some of technical specificities similar to the ones of the preferred option of this initiative.

Finally, the case study on pricing policy and estimation of potential VAT loss (in Annex 6) was drafted using a mock purchase approach.

10.6. Annex 6: Technical feasibility of the options

OPTION 1 – Status quo

Transmission of payment data to the tax administration

National competence through national processes.

Cleansing

The data have to be usable. For this, they must be linked to a usable tax identifier, which is assumed to exist nationally. Other processing is also necessary, such as aggregation of payments in a certain period of time.

Risk analysis

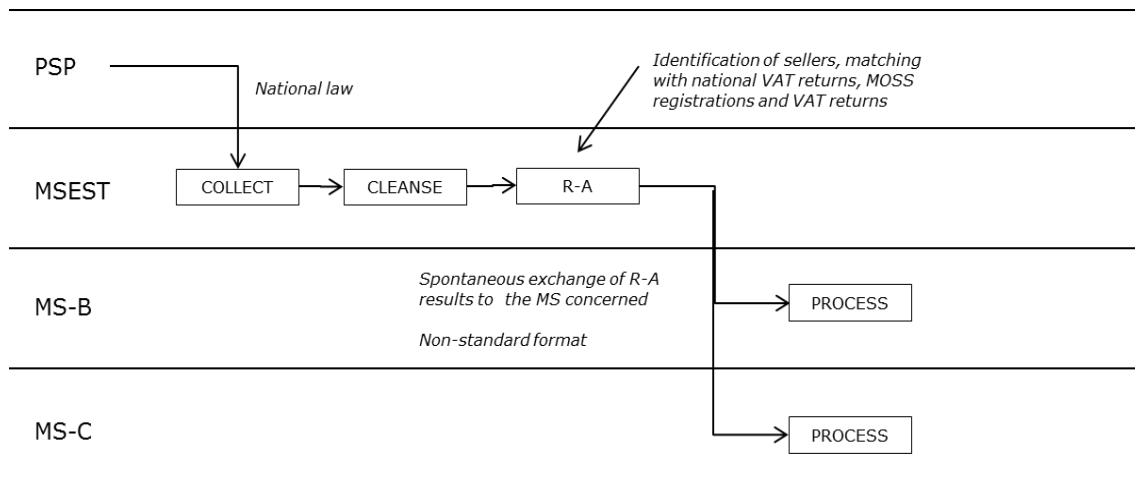
The data thus collected may be used to compare with other national sources, such as MOSS or VAT returns, turnover information, or other.

Store and exchange of data

Storage at national level. Specific cases that affect other MS may be sent spontaneously through administrative cooperation forms

Processing

MS can use payment data to carry out nationally VAT controls



PSP: Payment service provider
MEST: MS of Establishment of the PSP
MS-B: MS of the seller
MS-C: MS of the consumer
R-A: Risk analysis

OPTION 2 – non-regulatory

Transmission of payment data to the tax administration

As per option 1, But guidelines as regards the format of the data may be published.

Cleansing

As per option 1.

Risk analysis

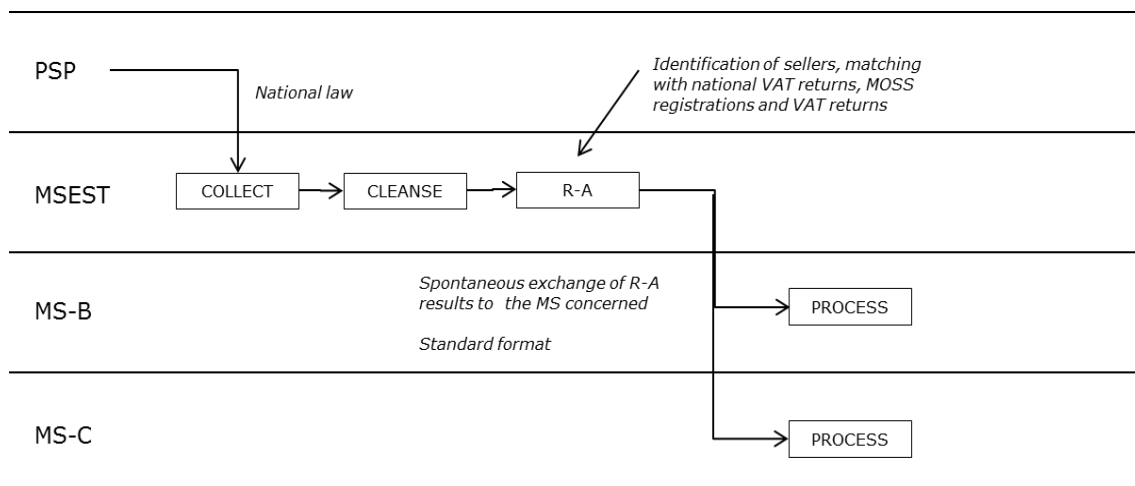
As per option 1.

Store and exchange of data

The form for the spontaneous exchange of information may be standardised

Processing

As per option 1



PSP: Payment service provider
MEST: MS of Establishment of the PSP
MS-B: MS of the seller
MS-C: MS of the consumer
R-A: Risk analysis

OPTION 3.1 – Distributed application (similar to the VIES)

Transmission of payment data to the tax administration

Transmission is to be foreseen in all MSs, by the PSP established in the Member States. The standardisation of the information received is necessary. The technical means for collection may differ per MS.

Cleansing

The data received by MSs need to be usable. *It is assumed that they contain an identifier for payees.* The data need to be cleansed (corrected) and organised per MS, where MS is the MS of the consumer (MS-C) or the seller (MS-B) in the payment record. The data then are stored and reorganised for dissemination.

Risk analysis

The aggregated data received per MS are used for risk analysis in comparison with other national sources, such a MOSS, VAT returns, turnover data etc.

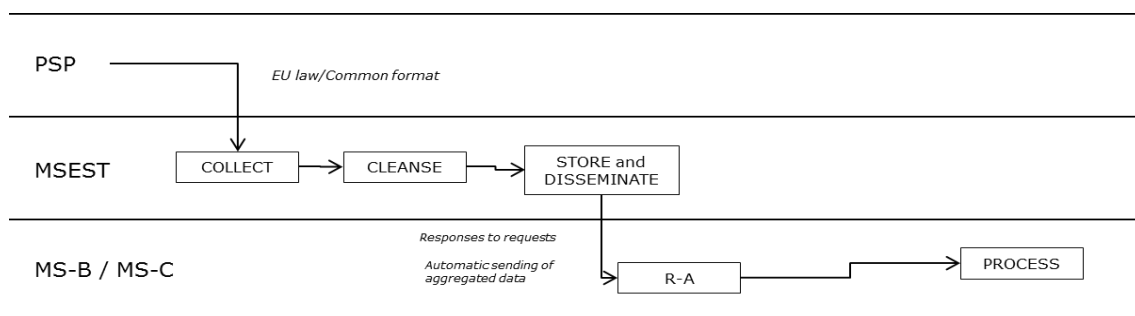
Store and exchange of information

In each MS, The data have to be stored per MS and reporting period a) as raw information concerning payees in that MS receiving the payment data or payees in other MS-B b) as aggregated information per reporting period per payee in the MS-B or having received payments from MS-C. The system has to a) send spontaneously aggregated information per MS and b) send the raw information based on queries specific to a payee.

This system is equivalent to the VIES recapitulative statements handling. It needs to use some form of validated identity for follow up queries to the detail of the information.

Processing and VAT audit

The result of the above analysis may give rise to specific administrative investigations and VAT audits. Such investigations may trigger receipt of further detailed payment raw data through the facility made available by the "store and disseminate" subsystem.



PSP: Payment service provider
MESTEST: MS of Establishment of the PSP
MS-B: MS of the seller
MS-C: MS of the consumer
R-A: Risk analysis

OPTION 3.2 – Central storage

Transmission of payment data to the tax administration

As 3.1. However, the data received are sent as such to a central location for the next processing step, the cleansing.

Cleansing

Processing taking place centrally.

The central system receives all raw data from all MS. *It is assumed that they contain an identifier for payees. Specific processing needs could be established to associate the identifier of the payees with a taxable person.* In such scenario, an **identity matching system** needs to be foreseen, which learns from experience (machine learning), from input of officials assigned to this identity matching and from results of the risk analysis process in MS, which may feed the identity matching system. In this system, the transmitted information is associated to one or many pieces of validated information, such as a VAT number. Following such processing, the data need to be organised per MS, where MS is the MS of the consumer (MS-C) or the seller (MS-B) in the payment record.

Risk analysis

At each MS, the aggregated data received per MS are used for risk analysis in comparison with other national sources.

Aggregation of data per risk indicators can be established (e.g. per amount of payments, number of payments, country of origin, country of destination....)

Store and sharing the information

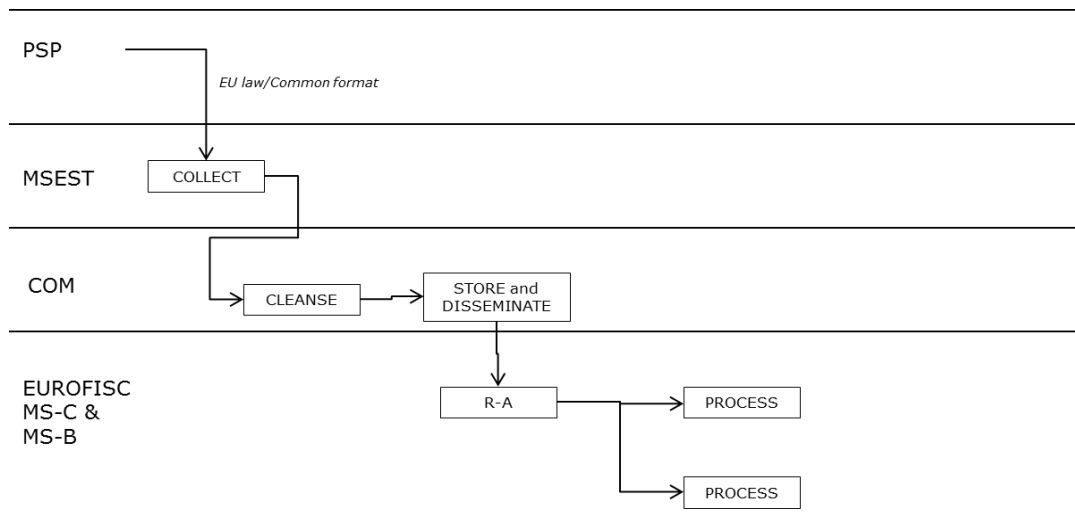
At the centre, the data have to be stored per MS and reporting period a) as raw information concerning payees per MS and b) as aggregated information per reporting period per payee in per MS.

The system thus created has to send spontaneously aggregated information per MS. Sending the raw information is not necessary, as this information is available centrally and may be accessed there only by Eurofisc officials of the Member States.

The system is using the identities produced by the identity matching system to calculate the aggregates. These records do contain also the basic information transmitted.

Processing and VAT audits

The result of the above analysis made at MS level may give rise to specific administrative investigations and VAT audits. Such investigations may use the central system to access the raw information. Thus, the central system must also be equipped to support the work of such investigations through appropriate definition and design. The data held centrally may undergo some processing specific to a limited set of traders, as they are identified from the national risk analysis operations. In addition, if national risk analysis has uncovered an identity of a trader, the identity matching system is updated.



PSP: Payment service provider
 MEST: MS of Establishment of the PSP
 COM: European Commission Central repository
 R-A: Risk analysis
 MS-B: MS of the seller
 MS-C: MS of the consumer

DESCRIPTION OF THE DIFFERENT STEPS

Transmission of payment data to the tax administration.

National collection from locally established payment service providers is considered not to represent a specific security challenge. These organisations are recognised formally in the MS of establishment and thus they have or may have standard working relations with the tax authority.

Cleansing

A fundamental aspect of cleansing is to make sure that the records received are usable. **In the particular case, each record must be able to be associated correctly to a taxable person.** In order to palliate this issue, we have introduced an **identity matching system.** This system is supposed to learn from experience: input of specific PSPs and of MSs' systems (e.g. the association of a reference received by one specific PSP with records received from other PSPs that may concern the same payee or validated identifications supplied from MSs).

From storage and processing perspective, the cleansing and the identity matching system will generate additional storage requirements and processing requirements where it takes place. The cleansing algorithms will most probably necessitate globally 3 times the storage of the basic information.

Store and exchange or sharing of information.

From a storage perspective, the centralised option has to be able to receive and store the +- 8 billion payment records annually. This represents a significant storage, in the range of +- 5 terabytes (5 thousands of billion characters) annually globally. The size of the transmission files is itself an issue and necessitates appropriate internet connectivity that we will consider available in all locations.

In the case of scenario 3.1, the data will need to be stored in each MS both in aggregated way per payee and raw no aggregated data. Data records will have to allow the identification of the payees (e.g. different registrations of the same payee in different payment systems). While aggregated data will be available to the other Member States electronically, raw data may be sent spontaneously. In the case of a centralised storage, the raw data will be available centrally for MS access. This information centrally is estimated in the range of 10 terabytes annually.

Risk analysis

The cross-match of payment data with other databases (as VAT, MOSS or other turnover databases) will be carried out by tax officials of the national administrations. In option 3.1 this will be done at national level, under options 3.2 this will be done at Eurofisc level

Processing and VAT audits

The centralised solution could develop other automated processes to allow further crosscheck of data, for instance with the VIES¹⁶¹. Such processing will generate additional storage needs.

The output of the risk analysis' output will be a number of targets to be further controlled by the tax authorities.

¹⁶¹ VAT Information Exchange System foreseen by Chapter V of Council Regulation (EU) No 904/2010

10.7. Annex 7: Case Study – pricing policy and estimation of potential VAT loss

The free nature of the Internet and the high degree of anonymity provided may make it easier to avoid VAT payment on B2C electronic transactions. The VAT loss is very hard to be determined and needs specialised audit tools, time, qualified skills, other important resources and comprehensive data, thousands of invoices and, above all, a competent authority.

However, it is possible to try to estimate the potential VAT loss using different proxies and an analysis based on out of ordinary pricing policy of different sellers. This exercise does not represent a valid proof of the VAT loss or VAT fraud to be used in courts, but still raising lots of legitimate questions.

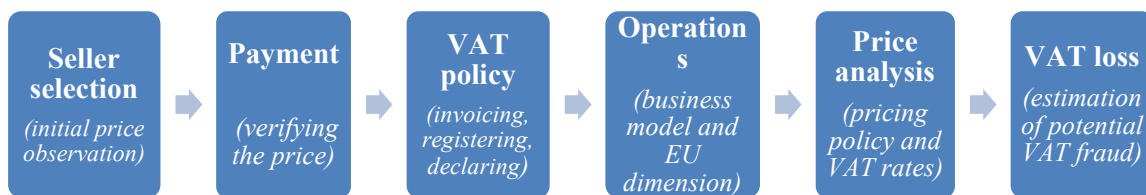
The estimation shows a **potential VAT loss of up to EUR 29 million for a 5-year period (EUR 5.7 million/year) from the one seller** we analysed in detail.

Methodological considerations

We used a mock purchase approach to reconstruct consumer experience from the initial moment of searching the internet for a product to the last click before the final purchase. We have tried to follow the process of buying a mobile phone¹⁶² from the internet.

Observation! This was as an exemplification only. We did not make any actual payment/purchase and no rules were broken during this exercise.

We tried to detect any anomalies in the selling price of the product and to analyse these discrepancies in order to capture any reasonable justification or to determine any indications (proxies) of potential VAT fraud. The illustration of our mock purchase exercise is here:



The findings were documented using free data sources (websites, forums, discussions, complains etc.). We tried to keep the estimation methods very easy to understand and to be as conservative as possible in our exercise.

We anonymised the real name of the seller, information that can lead to identification of the buyers and the data referring to other sellers. We kept all the evidence for our findings (lists, print screens, references etc.) to be able to defend our position, if needed,

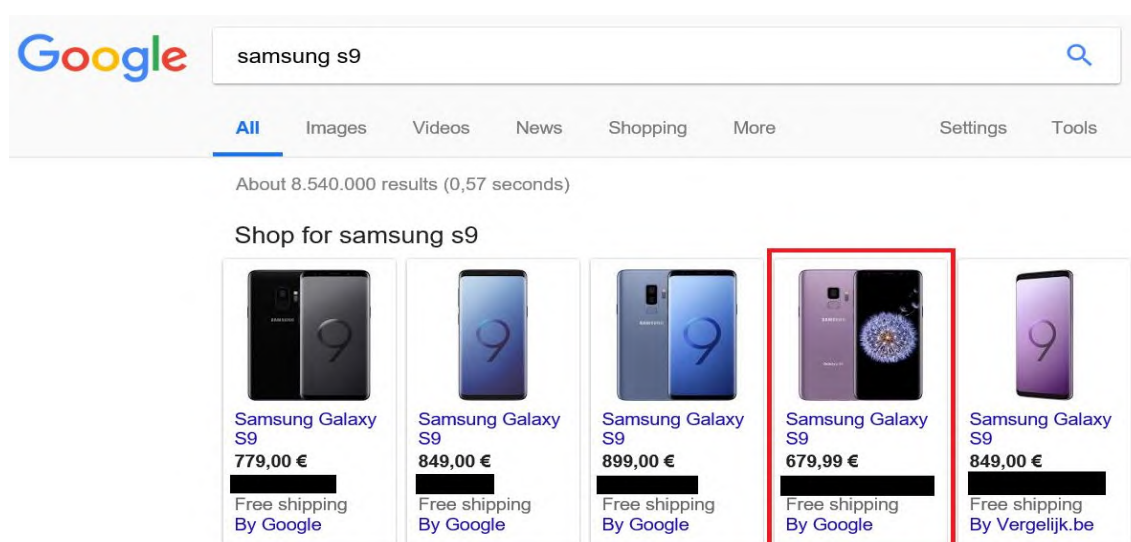
¹⁶² Our team selected the product based on what was “hot” when we initiated the search (19.03.2018). The product we used (Samsung Galaxy S9 phone) was just launched on 16.03.2018

and we validated our conclusions with EUROFISC¹⁶³, the EU's network of Member State VAT fraud experts.

1. Seller selection (finding the product and observing different prices)

Our team went online using the most popular search engine in the world¹⁶⁴ to find the product. The majority of new customers start the same way their search for a product.

Different factors drive purchase decisions. For our case, important aspects such as product features and brands are not determinant because we searched for the same product in different places. Price remains the main factor for the buying decision¹⁶⁵.



It is easy to **spot the lower price from the above** and we decided to **follow that specific seller**. We will further refer to this business as “The seller” in our case study.

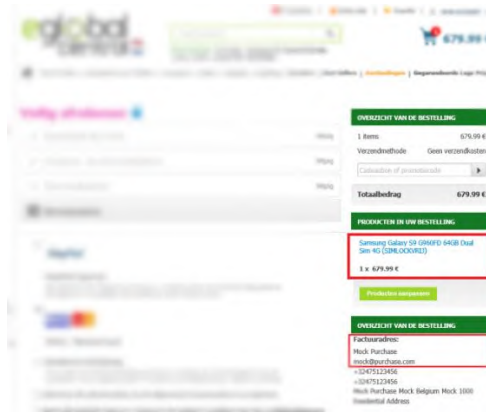
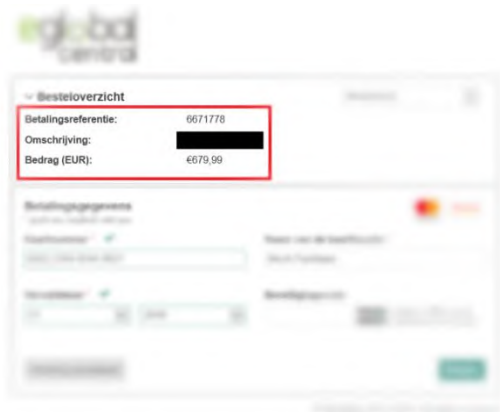
2. Payment (verifying the price)

We tried to see if the price is final or other taxes are added at a later stage of the process. Impersonating the average buyer, we (1) added the item to the basket; (2) proceeded to payment; and (3) verified the final price.

¹⁶³ EUROFISC is the European Network of National Officials specialised in combating VAT fraud. The EUROFISC network was established by Regulation on administrative cooperation and combating VAT fraud (Council Regulation 904/2010 (OJ L268 of 12/10/2010)) and officially launched on 10 November 2010

¹⁶⁴ Google has approx. 90% of the search engine market (<http://gs.statcounter.com/search-engine-market-share>)

¹⁶⁵ 2017 Global Online consumer report by KPMG (<https://home.kpmg.com/xx/en/home/insights/2017/01/the-truth-about-online-consumers.html>)



The final price corresponds to the listed price. There are no other taxes such as VAT or custom duties added to the listed price on the web shop.

3. VAT policy (invoicing, registering, declaring)

As this was an exercise, we did not make the real payment; therefore, we do not have the real invoice for this payment. However, we collected evidence (invoices) from different other sources: discussion forums, complaints, internet boards etc. We wanted to see if The Seller usually indicate any VAT on the invoices issued.

Our findings: different Member States, different invoices **and one point in common - no VAT** on invoices and no mention of any VAT and duties on the invoices. The example below shows anonymised invoices from customers in four different Member States: France (purchase made on .fr website operated by the seller), Germany (purchase made on .de website operated by the seller), Slovenia (.purchase made on .eu website operated by the seller) and Spain (purchase made on .es website operated by the seller).

France

FACTURE

Hong Kong
SITE WEB: <http://www.██████████.fr>
EMAIL: sales@██████████.fr

Post Office, 999077

Commande #5173613

STATUT: Expédié
DATE: 2014-12-16, 05:20
MODE DE PAIEMENT: VISA / MasterCard / Virement Bancaire
MODE DE LIVRAISON: Livraison Standard

Adresse de facturation:

██████████
MARSEILLE, Bouches-du-Rhône 13009
France

Adresse de livraison:

██████████
MARSEILLE, Bouches-du-Rhône 13010
France

Produit	Quantité	Prix unitaire	Sous total
Nikon AF-S DX NIKKOR 35mm f/1.8G Objectif Code: CLENNKN00042	1	145.99 €	145.99 €
		Sous total:	145.99 €
		Frais de Port:	0.00 €
			Montant total (Prix final): 145.99 €

Germany

DETAILS DER BESTELLUNG

██████████ (Germany)
██████████
WEBSEITE: <http://www.██████████.de>
E-MAIL: sales@██████████.de

Rechnungsadresse:

██████████
Leipzig, Sachsen 04357
Germany
+49.017.██████████
Adresstyp: ██████████

Bestellung #6561757

STATUS: Processed
DATUM: 2018-01-30, 21:47
ZAHLMUNGSMETHODE: PayPal Express
VERSANDMETHODE: Economy Express Versand

Lieferadresse:

██████████
Leipzig, Sachsen 04357
Germany
+49.017.██████████
Adresstyp: ██████████

Produkt	Menge	Stückpreis	Zwischensumme
Canon EOS 1300D SLR-Digitalkamera mit 18-55mm III Objektiv Kit Code: CDSRCAN00049M	1	276.99 €	276.99 €
		Zwischensumme:	276.99 €
		Versandkosten:	0.00 €
			Total Kosten: 276.99 €

Slovenia

Spain



INVOICE

(Europe)
Lai Chi Kok Road
Hong Kong
WEBSITE: <http://www.█.eu>
EMAIL: sales@█.eu

Order #6116767
STATUS: Dispatched
DATE: 2017-08-20, 21:21
PAYMENT METHOD: PayPal Express
SHIPPING METHOD: Insured Economy Express Shipping

Product	Serial No. & Lot No.	Quantity	Subtotal
Apple iPad Pro (2017) 10.5" 64GB Wifi Tablet - Silver Code: CTABAPP00210	Serial No: █ Lot No: DPO17016208	1	598.14 €

Subtotal: 604.99 €
Order discount: 6.99 €
Coupon: buybe4leave
Shipping cost: 12.10 €

Total cost: **610.10 €**



FACTURA

(España)
Lee Chung Street,
Chai Wan, 999077
Hong Kong
PAGINA WEB: <http://www.█.com.es>
CORREO ELECTRONICO: sales@█.com.es

Pedido #5116048
ESTADO: Enviado
FECHA: 2014-09-16, 20:16
MétODO DE PAGO: PayPal Express
MétODO DE ENVÍO: Económico Expres

Facturado a :

Daniel █
Toledo █
Spain █
+34 █
Tipo de dirección:

Envío a :

Daniel █
Toledo █
Spain █
+34 █
Tipo de dirección:

Artículo	Cantidad	Precio unitario	Subtotal
Genérico Kit de limpieza 5 en 1 para cámaras y objetivos Código: CCLTGEN00001	1	Gratis	Gratis
Nikon D5300 DSLR Digital Cámara con Objetivo VR II 18-55mm Kit (Negro) Código: CKITNKN00129M	1	529.99 €	529.99 €
SanDisk Ultra - Tarjeta de memoria SDHC de 32 GB (clase 10 UHS-I, 40 Mb/s) Código: CMEMSAD00024	1	Gratis	Gratis
Sony Tarjetas de Memoria 32GB 94MB/s SDHC Class 10 SF32UX Código: CMEMSON00010	1	33.99 €	33.99 €

Subtotal: 563.98 €
Gastos de envío: 0.00 €

Coste total: **563.98 €**

The “Terms & conditions” section on the websites of the seller mentions that the prices shown are final, without any other charges, supposedly including all taxes. The seller claims to have VAT included in the price. However, the seller does not appear to be registered in EU for VAT purposes and does not display a valid VAT number on any invoice. However, in the communication with its EU clients the seller admits he knows about its tax obligations. The seller claims to pay the VAT and customs duties. The e-mail below from the seller’s customer support (France and Belgium) perfectly illustrate this policy:

CS - Sales & Support <support@█> pour █ 16:07 | afficher les détails | répondre à tous <?> | davantage ▼

Le contenu distant a été masqué : toujours afficher le contenu distant venant de support@█ :

##- SWP n'écoutez pas sous cette ligne -##

Your request (41103) has been solved. To reopen this request, reply to this email.

CS - Sales & Support (█) (France & Belgium)
26 août 22:07

Bonjour,

Merci pour votre message.

Nous sommes au regret de vous informer que nous n'indiquons pas la TVA sur nos factures aux clients, car tous les droits de TVA ou de douane encourus sont payés par █ France.

Nous nous excusons pour les désagréments causés.

Si vous avez besoin plus d'informations, n'hésitez pas à nous contacter.

Cordialement,
█ (FR)

4. Operations (business model and EU dimension)

The seller uses multiple websites in different languages and different Member States:

AT	www.██████████.at (in German)
BE	www.██████████.be (in French)
DE	www.██████████.de (in German)
ES	www.██████████.com.es (in Spanish)
FR	www.██████████.fr (in French)
IT	www.██████████.it (in Italian)
NL	www.██████████.nl (in Dutch)
PL	www.██████████.pl (in Polish)
UK	www.██████████.uk.com (in English)
EU	www.██████████.eu (for the rest of EU)

The above websites try to create the appearance of a local website. However, the aforementioned web shops are just an interface for “drop shipping”¹⁶⁶. The seller receives and process the orders on these websites. A Hong Kong-based Ltd. company specialised in “drop shipping” sends the products to the customer.

Being able to evade the VAT and to offer very low prices is a game changer for any web shop: it boosts the sales and the merchant can make the same or even little more profit than compliant businesses in the same game with virtually no costs and little associated risks. In order to succeed and to worth the risk from the consumer part, the seller has to offer a very competitive (low) price. We will analyse this pricing policy in the next section.

5. Price analysis (*pricing policy and VAT rates*)

The seller offers very competitive prices on all its websites. The average discount indicated by the company on its websites is between 19% and 24% while the VAT rates are between 19% and 23%. Even if cannot be determined directly, the possible link between the very competitive (“*too good to be true*”) price displayed and the VAT rate can be easily noticed from the price analysis.

On top of the very low price, possible uncompliant sellers may benefit from other unfair advantages resulting from aspects such as no copyright issues, no return policy, no guaranty, no customer care department, and no legal costs. All these aspects offer a comfortable manoeuvre margin for the seller in terms of pricing policy.

Table 1: Price comparison in different Member States:

Member State	Seller's Price (EUR)	Market Average Price (EUR)	Seller's Discount (EUR)	VAT rate (%)	Seller's Discount (%)	Theoretical price in EUR (real price +	Potential price difference (EUR)	% Theoretical price difference (if theoretical
	167							

¹⁶⁶ "Drop shipping" is a legal retail fulfilment method where a store does not keep any stocks but purchases the item from a third party and sends it directly to the customer. The merchant never sees or handles the product. This business model usually operates with very low margins in a highly competitive niche market. Being easy to start the business with little or no overhead expenses, many merchants are involved in this type of business; selling prices are very close to the ones from the competitors. The little investment in getting started, usually low-quality websites and poor (if any) customer service, makes it possible to operate on tiny margins.

¹⁶⁷ As displayed on Seller's websites

	168					VAT)	VAT is included)	
AT	690	849	159	20%	19%	828	21	2,5%
BE	658	849	191	21%	22%	796	53	6,2%
DE	660	842	182	19%	22%	785	57	6,7%
ES	660	849	189	21%	22%	799	50	5,9%
FR	655	852	197	20%	23%	786	66	7,7%
IT	625	795	170	20%	21%	750	45	5,7%
NL	679	849	170	21%	20%	822	27	3,2%
PL	687	849	162	23%	19%	845	4	0,5%
UK	639	843	204	20%	24%	767	76	9,0%
EU	659	842	183	21%	22%	797	45	5,3%

On top of this, the company may benefit from other unfair advantages resulting from aspects such as no return policy, no guaranty, no customer care department, and no legal costs.

5.1. User experience (posts from customers on dedicated discussions forums)

User 1:

Registered User

Well that escalated quickly. It arrived today! Extremely efficient service and all is great so far, just charging the battery and reading a manual I downloaded from the canon site as mine is in Chinese. Camera was also in Chinese, mini heart attack averted by using a youtube video to show me how to find the language setting, it's in good old English now.

I didn't have to pay any import/VAT or anything, the invoice was labelled 'computer parts,' 18 euro... Those crafty Hong Konian bastards! 😊

User 2:

Registered User

UPDATE: ordered tuesday lunchtime. Picked up by DHL hong kong on wednesday. In my sweaty palm on friday lunchtime. Great price (150 euro less than ANYWHERE else) fast delivery. This crowd are legit. Will definitely order from them again.

BTW my "camera parts" were valued at 17 dollars for customs purposes!! 😊😊😊

1 person has thanked this post

User 3:

Registered User

Join Date: [redacted]
Location: [redacted], UK

Quote:
Originally Posted by [redacted]
Thanks all for the reviews. I've decided to risk the purchase of a Canon 60D. I'll let you know how it goes.

OK, I bought a 60D from HDEW and I wanted to leave a quick review of the experience:

- Response to email queries was very quick
- As they told me before buying it, the 60D is a grey import from the US (I don't mind)
- Price was very good: £729 including a free 3 year extended warranty
- Instead of the normal Canon warranty card you get an "XTEND Cover" card, and allows you to get the camera fi subject to pre-approval of the estimated quote

5.2. Additional questions (extension of the mock purchase exercise)

After this exercise, the main issue was to check if our findings are isolated (the product we search was on some kind of promotion or discounted), if the exercise is consistent

¹⁶⁸ Calculated as the average of best prices displayed by top selling companies in 5 Member States (UK, FR, DE, IT and ES)

(the findings can be extended to other seller) and widespread (if this practice concern other areas or is something specific to our chosen domain).

We tried to answer to the following questions:

- a. Is the seller applying the same pricing policy for other products on his websites?
and
- b. Are other sellers applying this policy on certain products?
- c. Is this practice affecting only electronics or other areas are also concerned?

a. Different products, one pricing policy

To answer the first question, we revisited the website(s) of the seller and compared the prices of other very popular products (based on customer’s preferences) with the average market price in EU¹⁶⁹. We found a 22% lower median price on the products compared. The full results are:

Selected Product	Seller’s price (EUR)	EU average price (EUR)	Price difference (%)
Apple iPhone X 256GB silver	969	1240	22%
Canon EF 100mm f2.8L Macro IS USM	649	869	25%
Apple MacBook Air 13.3 i5 1.8GHz 128GB	732	956	23%
Apple iPad 9.7" (2017) 32GB Wi-Fi	261	332	21%
Canon EOS 80D Body	699	974	28%
JBL Flip4	77	103	25%
Samsung Galaxy Tab S3 9.7 32 GB Wi-Fi	429	540	21%
Google Pixel 2 XL 128GB	789	990	20%
GoPro HERO6 4K	331	418	21%
Fitbit Charge 2	101	126	20%
Canon EOS 5D Mark IV Body	2359	3186	26%

b. 10 different sellers, same approach

To find an answer to our second question, we have selected the products with the biggest price difference and tried to verify the price with ten sellers mentioned on different forums to have similar practices¹⁷⁰. For the average user, these websites appear to be located in different EU Member States (Luxembourg, UK, France, Belgium, and Germany) but they mainly sell from outside of the EU (mostly China, but from United States also). Our results indicate a 23% lower median price for the first product and 21% lower price for the second product. The prices were between 19% and 28% lower than the average market price used for comparison. The table below shows the detailed price comparison (in EUR and %):

Seller	Product 1 (EUR)	Product 1 (%)	Product 2 (EUR)	Product 2 (%)
EU Average Price	974	100%	3025	100%
The Seller	699	28%	2359	22%
Alternative seller 2	708	27%	2347	22%

¹⁶⁹ We determined the EU price as an average of market prices in 5 EU Member States (BE/NL, FR, DE, IT, ES) taking into account the lowest selling prices displayed by biggest sellers on these markets (Fnac, MediaMarkt, Saturn, Amazon, eBay etc.)

¹⁷⁰ We anonymised the real names of the 10 sellers used for comparison

Alternative seller 3	789	19%	2326	23%
Alternative seller 4	793	19%	2545	16%
Alternative seller 5	781	20%	2427	20%
Alternative seller 6	763	22%	2400	21%
Alternative seller 7	687	29%	2223	27%
Alternative seller 8	669	31%	2195	27%
Alternative seller 9	769	21%	2459	19%
Alternative seller 10	740	24%	2431	20%
Price difference (median)	752	23%	2380	21%

c. Multiple areas may be affected by e-commerce VAT fraud competition

For the third question, we have seen evidence of the same price policy indicating possible VAT fraud in cross-border sales e-commerce in some other areas than the one we documented. Some of the main areas concerned are¹⁷¹:

- Textiles and shoes
- Electronics (computers, cameras, mobile phones, smartwatches, tablets, speakers etc.)
- Watches
- Videogames
- Television and broadcasting
- Beauty products (cosmetics, perfumes, etc.)

In relation with above areas, we found 40 other web shops and marketplaces with unusual price policies during our analysis. However, due limited time and resources available, we were unable to analyse these sites.

6. VAT loss (estimation of potential VAT fraud)

Our selected seller claims more than 500.000 customers: “*Seller has been providing online shopping services for more than 5 years and now we have a total of 9 online stores operated in Australia, the United Kingdom, USA, Germany, France, Spain, and Italy, which we have already served more than 500,000 satisfied customers*”¹⁷². We used a proxy related to the customer’s reviews to estimate the percentage of EU customers. Therefore, we analysed the dispersion of 26.806 reviews posted on *Seller’s* partner online review community. The results show that the large majority of reviews (more than 91% were written by people claiming they made their purchase from one of the EU Member States¹⁷³.

Country of the web shop	IT	ES	PL	FR	DE	UK	BE	AT	NL	EU	US	AU	Total
No of reviews	4272	3120	14	5064	1925	4653	688	426	1250	3139	854	1401	26806

¹⁷¹ These areas can be found in the list of most popular online purchases published by EUROSTAT http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals

¹⁷² www.██████████.eu/about-us-eu.html

¹⁷³ Own calculations based on Trustpilot reviews (www.trustpilot.com) posted at 19.04.2018

(%) of reviews	15,9%	11,6%	0,1%	18,9%	7,2%	17,4%	2,6%	1,6%	4,7%	11,7%	3,2%	5,2%	100%
----------------	-------	-------	------	-------	------	-------	------	------	------	-------	------	------	------

- Based on the listing prices of the top 150 most popular products (best sellers) we estimate the Average Order Value (AOV) at EUR 316 for the analysed seller. We took a very conservative approach, even excluding the top 5% expensive products from our estimation and assuming that the average customer bought only one product per purchase¹⁷⁴.
- **Our VAT loss estimate on this single seller is up to EUR 28.775.438 for a 5 year period (up to EUR 5.755.088 per year) at EU level**
- The seller extended its operation EU-wide over time; this business model clearly disturbs all EU Member States, even if the size of the potential damage for individual Member States vary significantly.
- The size of this potential fraud and the missing VAT remain unknown from the Member States.

¹⁷⁴ To estimate the AOV, we just rearranged the products based on their popularity and we analysed a potential basket with top selling 150 most popular products (over EUR 50.000, approx. 10% of all products available on the web shop). Due to the large sample and because at least top five best-selling products in each of the main 7 categories (cameras, mobiles, tablets, audio, gadgets, gaming, speakers) could be found in our estimation basket we have the reasons to believe that our the value of AOV used for calculation is reasonable. If we also considered the exclusion of most expensive products (possible outliners) from our calculation, we can conclude that we displayed a conservative estimation.

10.8. Annex 8: Result of the TAXUD 2016 survey on e-commerce compliance strategies in the EU

On 30 September 2016, the Commission DG TAXUD sent a survey to the fiscal attachés of the Member States to have an overview of VAT anti-fraud policies with a particular view on third party information. The survey was a follow-up of the Commission's VAT Action Plan where the Commission committed to address VAT fraud in the e-commerce sector.

The survey showed that in December 2016 only 50% of the respondent Member States¹⁷⁵ had a specific **e-commerce compliance strategy**. The e-commerce compliance strategy consists in participating in international and European events on e-commerce, monitor and examine new e-commerce trends, develop national cooperation or task forces between tax administration and mainly customs, but also with police and Consumer Rights Protection Agency, information campaign aimed at informing online traders of their tax obligations and consumers to recognise "risky" websites, supporting tax auditors, setting up e-commerce investigation and control projects.

The tax authorities with an e-commerce compliance strategy also have a **specific capability** (unit or team/task force) composed of tax auditors, IT experts and analysts in charge of VAT fraud in the e-commerce sector. Some of the Member States set up such specialised unit as a follow-up of the recommendations of the FPG038¹⁷⁶.

It should be noted that in the meanwhile Member States set up a new Eurofisc working field (N. 5) dealing with e-commerce. Also in this framework, different Member States delegations raised concerns regarding a clear legal basis to exchange VAT relevant data for e-commerce.

Another important issue is access to **third party information**. The survey showed that only 33% of the respondent Member States collect data from digital platforms established in their own jurisdiction (or with a branch) for VAT control purposes, while the percentage is 67% regarding collection of VAT relevant data from payment intermediaries. Only 5 tax authorities collect payment data from other national authorities monitoring money flows, such as financial investigation units in charge of anti-money laundering.

The information collected from **internet platforms** and the format vary from Member State to Member State and mainly refer to the identification of a given supplier, the taxable amount and the VAT number of a given supplier. Only in one Member State, the information is requested using a standard form.

However, even the Member States cooperating with internet platforms mentioned some criticality: the information is not always received or it is sent with a very long delay (even 6 months) or for a very limited period of time (shorted than the one subject to control). Often the information is not provided by the platforms because in the Member State requesting the information there is only a brunch of the platform while the information requested is owned by the main headquarters in another jurisdiction. Finally, the most recurrent problem is that when a tax administration asks for identification data of the suppliers the platform does not provide this information because considered as

¹⁷⁵ Twenty one Member States filled out and returned the questionnaire

¹⁷⁶ Fiscalis Project Group 38 on "control of electronic commerce"

"fishing" and against data protection regulation. Finally, only in 4 Member States traders selling goods and services through an account open online are obliged by law to make available online or to the tax authorities a tax identification number. This makes impossible to identify the taxable person behind a given web-shop.

When the platform is established abroad, the only way to receive information is through administrative cooperation. However, the information is not provided behind request of information (because the request is considered disproportionate – bulk request). Only 5 Member States reported to have received some spontaneous information from another tax administration under Regulation (EU) 904/2010 on B2C supplies from suppliers established in another Member State and taxable in requesting Member State.

The VAT Directive¹⁷⁷ allows Member States to hold third parties jointly and severally liable for payment of VAT. The questionnaire shows that this opportunity is used to a limited extent. Some countries, however, have general national regulations that entail VAT responsibility for internet platforms under certain circumstances. It should be noted that the new Article 14 of the VAT Directive introduced the deemed supplier provisions for the platforms at EU level as from 2021.

In 3 Member States, the tax administration has the legal authority to **shut down a web-shop** because of breaches to the VAT legislation, independently or in collaboration with another agency (i.e. consumer protection agency), but only one Member State reported to have used this possibility. However, the 57% of the respondent Member States indicated that in principle already the power of shutting down a web-shop/ IP address / web account (as such) could have a deterrent effect against VAT fraud. In fact, only this possibility may put some pressure on the traders to respect VAT obligations. Furthermore, as coercive measure this will result in a loss of reputation for a trader, will temporary stop the traffic of the seller (and the VAT loss for the treasury), and in general can be considered as a hurdle to fraudsters. On the other hand, other Member States do not consider this measure as an efficient anti-fraud tool, because traders can easily open another web account even with another identity or outside the EU.

Also for the **payment intermediaries** (such as credit cards, banks, financial institutions, currency agencies, digital and mobile wallet providers) the information collected vary from Member State to Member State and mainly refers to payments received by a given supplier from consumers in a Member State in a given period and to the identification of the recipients of the payments. Four Member States use a standard form to ask payment intermediaries for information.

Information exchange is a crucial tool for the Tax Administrations but problems occur when data is located outside the jurisdiction. Half of the Member States reported difficulties in receiving information from other jurisdictions.

¹⁷⁷ Council Directive 2006/112/EC Art. 205

10.9. Annex 9: Payment Services framework in the EU

Both payments services and payment service providers are defined and regulated in the European Union by the payment services Directive (PSD2)¹⁷⁸. The Directive is not restricted to euro transactions but applies to all payment services in all EU currencies within the EU, at both cross-border and national level. Furthermore, it covers third-party providers of payment services, such as payment initiation services offered in the context of e-commerce also when only one of the PSPs (involved in the payment transaction) is located within the EU.

Furthermore, the data and format standardisation of payment transactions is harmonised in the single euro payment area (SEPA). The SEPA territory also includes countries that are not part of the euro area and the EU¹⁷⁹. In particular, the SEPA Regulation¹⁸⁰ establishes the rules of an integrated market for electronic payments in euro, with no distinction between national and cross-border payments. The Regulation establishes wide requirements for credit transfers and direct debits in euro. In particular, it requires the use of certain common standards and technical requirements, such as the use of international Bank Account Numbers (IBAN), Business Identifier Codes (BIC) and the financial services messaging standards ISO20022 XML for all credit transfers and direct debits in euro in the EU.

Agreed standards, technical requirements and a common legal basis are the foundation for payments within the SEPA area, irrespective of the countries involved in the transaction. All Member States have migrated credit transfers and direct debits to SEPA.

It should be noted that the SEPA does not cover payments in other currencies. However, also other international systems such as SWIFT the global provider of secure financial messaging services¹⁸¹ use international standards like the ISO20222.

Credit cards schemes are not included in the SEPA regulation. However, the European Cards Stakeholders Group (ECSG)¹⁸² develops and maintains requirements and guidelines for cards. The "volume" (SEPA cards standardisation volume) defines general rules, functional requirements, data elements, security, conformance verification procedures, implementation guidelines for the cards schemes¹⁸³.

¹⁷⁸ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) OJ L 337, 23.12.2015, p. 35

¹⁷⁹ <https://www.ecb.europa.eu/paym/retpaym/paymint/sepa/html/index.en.html> It also applies to payments in euros in other European countries: Iceland, Norway, Switzerland, Liechtenstein, Monaco and San Marino

¹⁸⁰ Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 OJ L 94, 30.3.2012, p. 22

¹⁸¹ See: <https://www.swift.com/standards/about-iso-20022>

¹⁸² The ECSG is the industry association in charge of cards standardisation in SEPA. The ECSG is formed by representatives of five sectors of the card payments value chain: retailers/wholesale; vendors (card, payment devices, related IT systems); processors of cards transactions; card schemes and PSPs (represented by the European Payment Council)

¹⁸³ See: <https://www.e-csg.eu/scs-volume> the "Volume" has been published in March 2017 and the full implementation is foreseen by 2020

Finally, virtual currencies (VCs), better known as crypto-currencies, are not regulated in the European legal framework and in particular in the SEPA regulation and the PSD2. As such VCs are not in the scope of the regulatory option.

10.10. Annex 10: B2B import VAT fraud

It should be noted that import VAT fraud is sometimes combined with B2B schemes, where EU taxable persons import goods from third countries avoiding the payment of the VAT on importation and then re-sell the same goods (at a lower price) in the internal market. The case was documented in the “Bilton’s Bargains – The Billion Pound VAT Scam” programme, where BBC journalists documented the VAT fraud by impersonating a Chinese seller on eBay and Amazon and importing goods smuggled into the EU without paying VAT¹⁸⁴.

In particular, goods can be introduced in the internal market avoiding the payment of VAT by using Missing Traders fraud. Fraudulent businesses (missing traders) import goods from outside the EU pretending to transport and sell them to other businesses in a Member State different from the one of importation. In this way, these companies can benefit from a VAT exemption upon importation¹⁸⁵ (using particular procedures such as customs procedures No 42 and 63), and are supposed to declare and pay the VAT in the Member State of final arrival of the goods. However, in reality, the goods are placed in a fulfilment centre in the EU and sold on the black market. Then the fraudulent company just disappears without remitting the VAT to the tax authorities¹⁸⁶. This simplification regime was introduced in the VAT Directive in order to allow for transit of goods in the internal market without imposing unnecessary VAT burden to the traders¹⁸⁷. This procedure is widely used by legitimate businesses¹⁸⁸ but there is also evidence of abuse in order to introduce goods into the internal market with no VAT payment¹⁸⁹.

The customs procedures No 42 and 63 are two VAT regimes provided for by Article 143(1) of the VAT Directive that allow for a VAT-free importation of goods by a taxable person in a Member State if it is followed by a VAT-exempted supply or transfer to a taxable person in another Member State.

¹⁸⁴ See: <http://www.bbc.com/news/business-42143849>

¹⁸⁵ In 2015, there were 8.5 million import transactions with a VAT exemption, with a total value of EUR 74 billion

¹⁸⁶ In the European Court of Auditor Special report no 13/2011, it was mentioned that for 2009 by extrapolation the level of VAT losses in relation to cpc42 only would approximately reach EUR 2.2 billion. Report SWD(2017)428 final of 30.1.2017 impact assessment accompanying the document Amended proposal for a Council regulation Amending regulation (EU) No 904/2010 as regard measures to strengthen administrative cooperation in the field of VAT, p. 23-24

¹⁸⁷ In principle, an import of goods should be subject to VAT and this input VAT reported and offset in the VAT return of the importer. In normal scenario, the importer will sell the goods in the same country enabling a compensation of import VAT (input VAT) with the VAT on the sales (output VAT). However, in case the importer does not have VAT taxable transactions in the country of importation compensation of input VAT with output VAT is not possible. The importer will need to request a reimbursement of the VAT to the tax authorities and is then supporting the burden of financing VAT while in the end no VAT is due in the Member State of importation. To compensate for this situation, a VAT exemption on importation of goods that are transiting to other Member States has been introduced. It improves the cash flow situation of businesses and reduces their administrative burdens.

¹⁸⁸ SWD(2017)428 final of 30.1.2017 impact assessment accompanying the document Amended proposal for a Council regulation Amending regulation (EU) No 904/2010 as regard measures to strengthen administrative cooperation in the field of VAT, p. 25

¹⁸⁹ See: <http://www.bbc.co.uk/news/business-34650014>;

and: <http://www.theguardian.com/business/2015/nov/01/uk-losing-millions-vat-non-eu-sellers-amazon-ebay>

One weakness is that the entire process can take a long time to check, despite the risk of fraud occurring quickly. In particular, the correct control of these procedures depends on the effective cooperation between tax and customs authorities.

A specific new provision is included in the 2017 Commission proposal to amend Council Regulation (EU) No 904/2010 as regard measures to strengthen administrative cooperation in the field of VAT¹⁹⁰ in order to give tax authorities of the Member States of destination of the goods access to the relevant customs information submitted in the Member States of importation. Furthermore, the customs authorities will have access to VIES information in order to check the conditions for the VAT exemption in line with Article 143(1) of the VAT Directive.

¹⁹⁰ COM(2017)706 final

10.11. Annex 11: Third countries using payment data as VAT control tool

Some non-EU countries are using payment service data as a tool for detecting non-compliant traders in combination with simplified collection regimes for cross-border B2C supplies of goods (similar to the EU system).

In **Australia**,¹⁹¹ the Tax Office (ATO) can access some credit card transactional data where payments are going overseas and can also source some aggregated transactional data on credit card payments to identified non-resident suppliers. It is also actively identifying other third party transactional data sources as payment methodologies evolve¹⁹². The provided information refers to the identification of the supplier and on the amount of the transaction. This transmission is electronic and the information stored in electronic databases of the TAO that allows authentication of the information and of the sender, confidentiality (the communication can only be read by the intended recipient), integrity (the transmission cannot be altered) and non-repudiation (there is a record of the transmission and content).

Norway introduced a simplified registration system for VAT on electronic service (VOES) in 2011 (similar to the EU MOSS). Service providers without a place of business or establishment in Norway providing electronic services to clients other than businesses and public authorities in Norway may opt for a simplified registration and declaration of VAT (instead of registering through an intermediary). Furthermore, third parties such as payment intermediaries' are obliged upon request to give the tax authorities information that can be relevant in determining a taxpayer's tax obligations¹⁹³. Third party data, information, must be available on demand and in a format satisfying legal requirements.

Finally, also in the **United States** all US payment processors are required by the Internal Revenue Service (IRS) to provide information about certain customers who receive payments for the sales of goods or services¹⁹⁴.

¹⁹¹ As from 1 July 2018 the overseas suppliers to Australian consumers will have to register, collect and remit the GST for low value imported goods (goods of a value of \$ 1.000 or less purchased by consumers in Australia from overseas suppliers with Australian sales of \$75.000 or more). The registration, collection and remittance of GST is a responsibility of the online marketplaces if they facilitate the taxable sales.

¹⁹² The Taxation Administration Act 1953 (TAA 1953) Section 396-55. See: <https://www.ato.gov.au/law/view/document?docid=PAC/19530001/Sch1-396-55>

¹⁹³ Lov 27. May 2016 nr. 14 om skatteforvaltning (Skatteforvaltningsloven) The Taxation Administration Act

§ 10-2 https://lovdata.no/dokument/NL/lov/2016-05-27-14/KAPITTEL_10#KAPITTEL_10

¹⁹⁴ <https://www.irs.gov/pub/irs-pdf/i1099k.pdf>

10.12. Annex 12: Visual examples of the regulatory options

The table below shows a simplified example of the payment data that will be transmitted under the regulatory options (sub-option 3.1 and sub-option 3.2) by the PSPs to the tax authorities where they are established

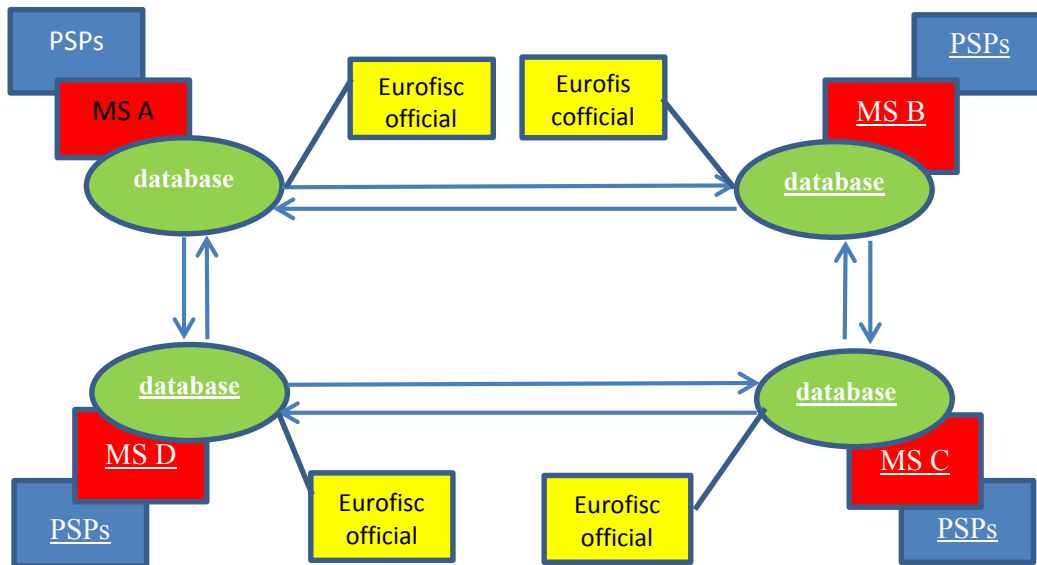
Table 8: Simplified example of payment data transmitted to a Member State from the Payment Service Providers established in that Member State

Payee (the beneficiary of the payment) identifier: and location	Reporting period	Origin of the payment	Payments transactions in the reporting period	Payment transaction identifier	Description of the supply underlining the payment transaction (if available)
Id: Mickey Mouse Tax number (if available) Location: Wonderland	Q1 20XX	Member State A	EUR 25 in date xx/xx/xx	Xxxxxx	Mobile phone
Id: Mickey Mouse Tax number Location: Wonderland	Q1 20XX	Member State A	EUR 30 in date xx/xx/xx	Yyyyyyy	Music
Id: Mickey Mouse Tax number Location: Wonderland	Q1 20XX	Member State B	EUR 15 in date xx/xx/xx	Zzzzzzzz	Book
.....

After the transmission of data from the PSPs, the tax authorities must exchange the data.

The figure below shows how payment data can be exchanged under the distributed system (sub-option 3.1)

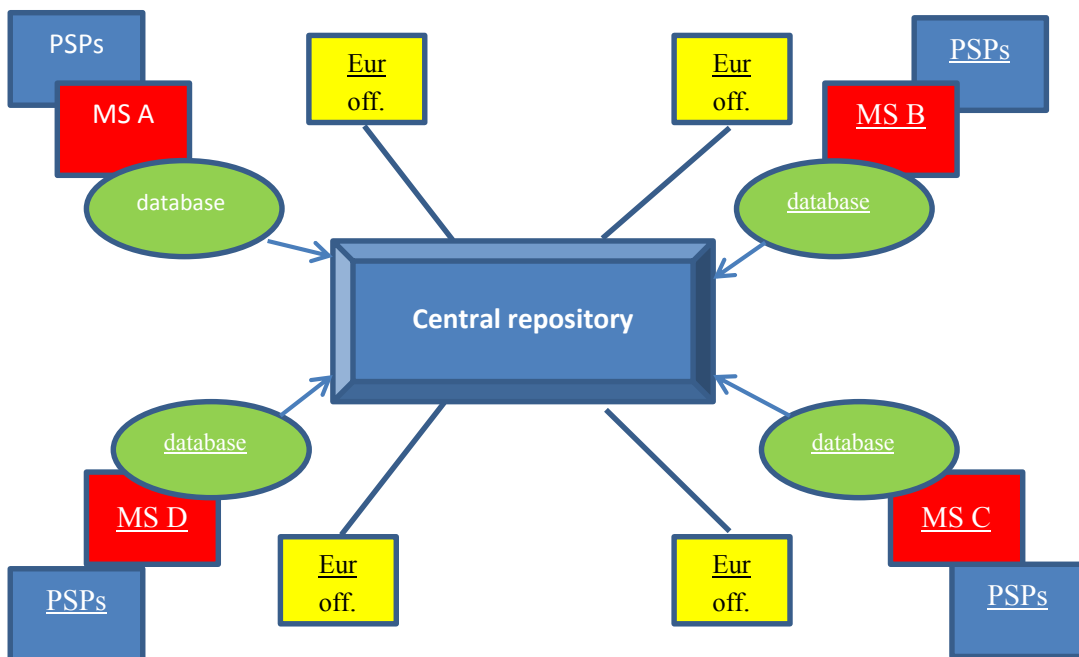
Figure 21: Distributed application exchange of info



The payment service providers (PSPs) transmit payment data to the tax administration of the Member State (MS) of establishment. The MS of establishment stores the data in a national database that is connected to the other national databases of tax authorities through a distributed application. Only the Eurofisc officials (Eur. Off.) will have access to payment data referring to their own MS.

The figure below shows how payment data can be shared through the centralised database (sub-option 3.2)

Figure 22: Central repository of data



The payment service providers (PSPs) transmit payment data to the tax administration of the Member State (MS) of establishment. The MS of establishment stores the data in a national database and then upload the data in a central repository. Only the Eurofisc officials (Eur. Off.) will have access to payment data referring to their own MS

In the targeted consultation PSPs and tax authorities were also asked whether alternative technical solutions could reduce costs or make the transmission and exchange of payment data easier.

One solution was to give the payment service providers established in the EU the option to choose one single Member State (even different than the Member State of establishment) to transmit all the VAT relevant data on inbound and outbound payments. This solution was basically conceived to permit payment service providers with different branches in different Member State to transmit the payment data to one single tax authority. Another solution was to give the possibility to payment service providers to upload payment data directly in the central repository and skip the first step (transmission of data to the tax authority in the Member State of establishment). The stakeholders were unanimous in discarding these solutions. The main problems refer to data protection issues and legal uncertainty. Therefore, these variants have not been taken into account

10.13. Annex 13: Comparison amongst different initiatives in terms of fighting e-commerce VAT fraud

The table below summarises the impact on VAT fraud of different initiatives as described more in detail in section 6.2.1 of the report.

Table 9: Comparison amongst different initiatives in terms of fighting e-commerce VAT fraud

e-commerce VAT fraud patterns		No VAT registration	No VAT declaration and payment	Under-declaration Of imports of goods	Mis-description of the import of goods	VAT declaration in the wrong place for distance sales (intra-EU) of goods
Initiatives addressing e-commerce VAT fraud	Exchange of payment data	Fully addressed	Fully addressed	Fully addressed	Fully addressed	Fully addressed
	Abolition distance sales threshold And extension of the MOSS (intra-EU)	Partially addressed: the distance seller can still remain in the black market and supplying abroad without any registration	Partially addressed see previous box	Not applicable	Not applicable	Partially addressed: the supplier can still potentially declare in the wrong place exploiting the new EUR 10.000 threshold
	Abolition small consignments exemption (imports from outside the EU)	Not applicable	Not applicable	Partially addressed: it is still possible to declare less in order to pay less VAT	Partially addressed: imports can be still declared as gifts or c2c or samples	Not applicable
	IOSS (import of goods from outside the EU)	Registration under the IOSS will be optional (voluntary compliance measure)	Again IOSS will be an optional system	Partially addressed: the under-declaration is still possible to pay less VAT	Partially addressed: still imports can be declared as gifts or c2c	Not applicable
	Deemed supplier	Partially addressed: only certain platforms are covered and only goods sold through the platforms	Partially addressed: see previous box	Partially addressed: only goods under the customs thresholds sold through the platforms	Partially addressed: see previous box	Partially addressed: see previous boxes