Payment Data in VAT/GST Risk Management:

- Sources
- Reliability
- Use in Compliance

Tim Renner – VAT Adviser, OECD VAT Unit
IOTA Forum on Combating VAT Fraud – Tbilisi, Georgia, 6-7 May 2026

BETTER POLICIES FOR BETTER LIVES

Background

- WP9 Focus Group on VAT/GST Enforcement
- Detection strategy – follow the money
- Payment data crucial
- Increased interest in payment data reporting regimes
- Lack of understanding among tax administrations as to what is available, who has it, how reliable is it, and how to use it
- Launch of the VAT Consultative Project on Payment Data (VAT – CPPD)
- Tax administrators and payment industry experts working together

VAT – CPPD Objective

- Develop guiding principles & identify practical considerations for the effective & efficient design & operation of payment data reporting approaches, through:
  - Ensuring a proper understanding of the payment ecosystem in digital trade.
  - Identifying opportunities to maximise the operational efficiency of payment data reporting requirements.
  - Considering options to minimise compliance costs and administrative burden and safeguard data security and privacy.

Relevance of the work beyond reporting regimes

- Not all jurisdictions are ready or willing to commit to a payment data reporting regime
- However, they need access to payment data to support compliance programmes
- This work allows them to target data acquisition activities appropriately to maximise results
- Through domestic information gathering powers or, through Exchange of Information requests with other jurisdictions

Outputs to date – general guiding principles

1. **Evaluate the need for introducing payment data reporting requirements** for payment industry actors **to complement** a broader VAT compliance risk management strategy**.**

2. **Have a clear understanding of the pursued policy objective**.

3. **Consider interaction** of the envisaged payment data reporting requirements **with the jurisdiction's overall VAT/GST compliance management framework/strategy**, including other reporting obligations.

4. **Have a proper and up-to-date understanding of the operation of the payment ecosystem** in digital trade and of the role(s) of different actors involved therein.

5. **Consult with stakeholders concerned/involved** from the outset of the process to ensure a good understanding of their business processes and available payment data and to establish the appropriate environment in a workable and proportionate manner.

6. **Leverage on (or develop) a robust legal framework** that ensures accessibility to the required data under strong safeguards aligned with other regulatory requirements, notably data privacy, data protection and financial secrecy legislation.

7. Design the reporting requirements to **strike an appropriate balance between administrative and compliance costs** while **minimising disruption**.

8. **Regularly monitor and evaluate** the efficiency and neutrality of reporting approaches, including their potential impact on the evolution of other payment methods in digital trade.

Outputs to date – emerging observations

- Relevant payment data for VAT/GST compliance risk management are typically dispersed across multiple entities in the payment chain.
- There is typically no single data point enabling reliable and straightforward traceability of a payment from a customer (payer) to a supplier (payee; merchant) throughout the payment process. A combination of data points often held by various entities in the payment chain is required.
- Availability of relevant payment data to an actor may not necessarily translate into a straightforward reportability of these data.
- Payment-related information is typically available at an aggregated level and tends to lack sufficient detail on aspects that relate to the nature of the underlying supply and/or the status of the parties involved for VAT purposes.
- The reliability and quality of available relevant payment data can vary significantly among actors in the payment chain.
- Particular sensitivity concerns may arise due to privacy and data protection regulations or internal operational constraints.

Outputs – Mapping Available Payment Data - extract

	Entity type[5]				
Data linked to	**Card scheme**	**Issuer bank**	**Acquirer bank**	**Payment processor[6]**	**Marketplace/Digital platform**
Payee (Merchant)	• Merchant name assigned by the acquirer bank • Merchant ID • Country code • Merchant category code • Address • Bank name – Interbank Card Association Number	• Merchant name[7] • Merchant ID • Merchant country • Merchant category code	• Name[8] • Merchant name • Merchant ID • Merchant category code • Address • Bank name • Bank location • IBAN • Billing address • Phone contact • Email address	• Name – legal name and name of account holder into which funds are deposited • Merchant name • Merchant ID • Other ID – government issued ID (e.g. passport, driver's license, tax identification number for certain countries) • Country code • Merchant category code • Address • Bank name and location	• Name – legal name • Merchant name – trading /commercial name, if different from legal name • Merchant ID • Country code – linked to business address (not the code linked to bank account where funds are disbursed) • Address – business address • Bank name* • Bank location*

Source: OECD WP9 Secretariat

Outputs – Payment Data Evaluation Framework

Scale	Accessibility	Reliability	Quality	Sensitivity
High (H)	**Direct access** – the actor has first-hand, unrestricted access to the original source of the data.	**Highly reliable** – data is consistently available, stable over time and produces the same or highly similar results when measured or observed multiple times. It demonstrates consistency and repeatability.	**High quality** – data is accurate, complete, correctly formatted, complies with required rules, and is free from corruption.	**Highly sensitive** – data is confidential, personally identifiable, or regulated under data protection and privacy regulations.
Medium (M)	**Limited access** (via third party) – the actor does not obtain the data directly but receives it from another actor(s).	**Moderately reliable** – data is generally available and stable but may occasionally show discrepancies or minor errors. While it is mostly repeatable, some variations may occur across different observations or measurements.	**Moderate quality** – data is mostly accurate and complete but may have some inconsistencies, minor formatting errors or missing details. While the data is usable, it may require some validation, cleaning, or correction.	**Moderately sensitive** – data is not strictly confidential but still subject to some privacy or internal business restrictions.
Low (L)	**Restricted access** – the actor can only access partial or indirect data, often restricted due to regulations, or privacy concerns.	**Unreliable** – data is inconsistent, unstable, and prone to significant discrepancies or errors.	**Low quality** – data is incomplete, or frequently incorrect or in a format that makes it difficult to use. It may require substantial cleaning and validation.	**Low sensitivity** – data is not confidential, posing minimal privacy and security concerns.

Source: OECD WP9 Secretariat

Outputs – Payment Data use in Compliance

Available payment data elements with relevance for VAT compliance risk management

Data linked to	Relevance for VAT compliance	Examples of data points
Payee (merchant)	Identification of the payee (merchant)	• Merchant name, including 'Doing Business As' (DBA) name or trading name. • Merchant identifier assigned by different actors in the payment chain, including: Merchant ID (MID); Card Acceptor ID (CAID); Commerce ID. • Government-issued identification numbers including the VAT registration number, other tax identification number (TIN) or business registration number linked to the merchant. • Country (postal address associated with the merchant's business) where the merchant is registered/operates. • Merchant bank account data including International Bank Account Number (IBAN) indicating the merchant's account number used for settlement of funds; Bank Identifier Code (BIC/SWIFT Code) identifying the financial institution where the merchant's bank account is held. • Other merchant information, such as email address, phone number, website URL.

Source: OECD WP9 Secretariat

Thank you