BORDERLINK

POLICY BRIEFING

The risk of risk management: Combinations of data sharing barriers are the biggest barrier for customs interoperability

Dr Duncan Shaw, Dr Ashutosh Sharma,
University of Nottingham

September 2026

Contact: duncan.shaw2@nottingham.ac.uk

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

UK Research and Innovation

© BORDERLINK Project – All rights reserved

Executive Summary

The European Commission's customs reform package, tabled on 17 May 2023, describes a customs union whose integration depends on a of scale data sharing that currently does not exist. The new EU Customs Authority is a single centralised IT environment that is intended to replace the fragmented landscape of 27 national customs IT systems. But to implement the new EU Customs Authority (EUCA) and the EU Customs Data Hub a significant gap must be bridged, between general support for increased data sharing between customs organisations, and the relatively low scale of how it is done now. Much more data could and should be shared. This is a key reason for implementing EUCA. The need to share more data also applies to customs organisations outside of the EU because the nature of customs work is border-crossing. Here we investigate this tension and potential solutions.

From our interviews and documentary research we have found that the fundamental problem with data sharing is that individual data sharing barriers combine in complex ways to make it difficult to judge the risk of authorising or sharing data to separate organisations for the first time. This makes the *perceived* risk too great to authorise, or maybe even to ask for, when considering ad hoc analyses. Ad hoc analyses are non-standard, speculative or non-routine analyses that are customised to progress individual investigations, and they also lead to developing routine, standardised and larger scale methods.

The perceived complexity of the risks of data sharing, and the potential consequences for anyone who authorises such sharing, are the real barriers to data sharing. The data sharing barriers and risks are different for every bilateral sharing relationship – and even in each direction – but they are drawn from a single set of risks and barriers and they are not interdependent. *They are merely complicated not complex. It is possible to better understand the risks of each potential data share to the sharing organisation and to the authoriser.*

We develop a simple method of assessing the risks of sharing based on a Data Trail Model (DTM) and a Bilateral Asymmetric Data Sharing Model (BADS). This method also helps analysis to assess which data sources to approach for which data and what the benefits are of doing so.

The DTM model helps analysts to visualise what new data and data sources might be available. It connects direct and indirect entities, journey stages and super stages, past records and future expectations, organisational perspectives, organisation data sources, supply chains levels of analysis and the data trails that are produced by entities' behaviours as they travel. This enables

customs analysts to choose abstract low risk data which still helps an investigation to progress but is easier to request from sources to initiate new data sharing relationships. The BADS model helps potential data source organisations to assess the risks of sharing different data with different requestors. Together the two models support increased data sharing by reducing the perceived risk of sharing and by increasing the number of options for what data to use and what sources to get it from, which also improves data analysis strategies.

Next, we will continue to validate and extend the ideas and methods mentioned here in a discussion process to raise awareness of these solutions, to form consensus and to potentially support the design of the EUCA, specifically in the planning of Risk Management Operations.

Table of Contents

1. Introduction 6
1.1. This policy paper 6
1.2. This paper's place in the BORDERLINK project 6
1.3. Paper overview 6
2. Policy and Regulatory Considerations – The policy problem and its implications 7
2.1. The problem with data sharing 9
2.2. The support for more data sharing, precedents and examples 10
3. Data sources used in this research 16
4. 4. Strategic Alignment with the EUCA Mission – Why Customs needs more data sharing . 17
4.1. Reason 1: Interoperability and how a system function 17
4.2. Reason 2: New data enables new decisions and new actions 17
4.3. Reason 3: New AI technologies require more data sharing 22
5. Data sharing barriers 23
5.1. Types of data sharing barriers 23
5.2. Data sharing barriers are either 'blocks' or 'gaps' 26
5.3. Data sharing is always bilateral and directional 26
5.4. Risky barrier combinations are the fundamental challenge 28
6. Key findings: How to reduce the risk of risk management data sharing 30
6.1. Key Finding 1: The Data Trail Model – Visualising the big picture of direct and indirect data trails 30
6.2. Key Finding 2: The BADS model – Understanding data sharing relationships between organisations 31
6.3. Key Finding 3: Checksum-based data sourcing strategy – Kich-starting the data sharing journey 33
7. Conclusions 36

Table of Tables

Table 1: Different types of barriers to data sharing with examples. Datasets are collections of data of any type and size. Data senders and receivers are usually in separate organisations, but this is not always clear, e.g. when legal powers or access to capacities and capabilities vary across an organisation. Or when a single government is considered to be a collection of separate ministries and other separate agencies. Includes sender and reivers in the same country and part of the same government, as well as international data sharing. 26

Table of Figures

Figure 1: The Big Data Information Value Chain: How data, information, knowledge, decisions and actions relate to each other 18
Figure 2: Physical journeys are made up of many stages, and each stage produces a data trail on an "information journey" 19
Figure 3: An entity's journey generates a bundle of overlapping data trails: the vehicle trail, the trailer trail, the driver trail, the cargo trail, the pallet trail and other entities 20
Figure 5: (a) Each bi-lateral share is different with different combinations of barriers and benefits, A to B ≠ A to C. Also, the barriers and benefits are different in each direction A to B ≠ B to A. (b) Indirect reciprocation is more likely to be beneficial than direct reciprocation because there are more sources to receive from, so there is a greater range of potentially valuable data. A and B have different data and data requirements but C's priorities 'complete the equation'. 28
Figure 4: The Data Trail Model (DTM) helps analysis decide which data is required and where it might be sourced from because it combines journey stages and super stages, organisations that have different levels of perspectives and the data trails that different direct and indirect entities produce as journeys progress. 31
Figure 6: Combinations of barriers between data senders and receivers are complicated not complex. They only scale linearly with additional senders and receivers – risks can be assessed at each bilateral level rather than the level of a whole network of senders and receivers. There are a limited number of combinations of barriers, different in each direction, but with many in common. 33

1. Introduction

1.1. This policy paper

This working paper was written to describe our research on problems in sharing data between customs organisations and to test some solutions. Data sharing is important because it is the fundamental enabler of interoperability between customs organisations, which is a basic objective of the BORDERLINK project. Also, data sharing and interoperability will be fundamental to the successful operation of the new EU Customs Authority (EUCA).

1.2. This paper's place in the BORDERLINK project

The research that led to this paper was part of the Data Management Plan (DMP) deliverables of the BORDERLINK project[1] (the two plans are D1.2 and D1.3). The initial DMP included a questionnaire of consortium members to monitor their use of data in the project and any problems that they encountered[2]. A main finding of the DMP questionnaire was the existence of data sharing barriers. For example, problems in sharing data between customs organisations involved in the Inland Waterways component of the BORDERLINK project, which involved countries along the banks of the river Danube. These data sharing problems were not major obstacles for the project's deliverables, and the Inland Waterways problem was later solved by the consortium members involved, but this incident first highlighted the critical nature of data sharing in supporting customs interoperability and the project's deliverables. Also, promoting interoperability in general between European customs organisations was a fundamental aim of the BORDERLINK project.

On further investigation it became clear that there was a fundamental tension between the strong need, and widespread support, for data sharing between customs organisations and the barriers to doing so. This tension appeared to be a significant barrier to the project's deliverables around sharing data and interoperability, and a policy problem for implementing the new EU Customs Data hub. Therefore, we investigated further and this paper reports our findings so far.

1.3. Paper overview

This paper starts with an overview of the policy problem caused by the tension between a widespread support for more data sharing between customs and the barriers to doing so. Next the paper explains the fundamental reasons why customs organisations should share more

[1] Project website: https://www.borderlink.eu/about

[2] D1.2 Data Management Plan Version 1.0, November 2025. Over the course of the project the two DMPs will generate three DMP questionnaires.

data. Then the paper describes the many types of data sharing barriers, how they combine and how these combinations make sharing so difficult – because the bewildering combinations make it seem impossible to calculate the risks of authorising or sharing data. This is the risk of risk management data sharing.

Next the paper describes how to reduce this risk and therefore unblock data sharing, by using two models. The first model is the Data Trail Model, a method of visualising the big picture of direct and indirect data trails that are generated when all entities travel. The second models is the BADS model, a simplified method for understanding data sharing relationships between many organisations.

Finally, the paper describes our conclusions and suggestions for next steps.

2. Policy and Regulatory Considerations – The policy problem and its implications

The EU parliament's reform of EU customs moved forward in March 2026 with the Council and the Parliament agreeing to create a new EU Customs Authority (EUCA). The EU Customs Authority will coordinate and support national customs authorities across the EU, with responsibility for EU-level risk management, identification of priority control areas and risk criteria, and EU-level crisis management. A major enabler for this will be the new EU Customs Data Hub.

The EU Customs Data Hub is designed to:

"- collect and analyse customs data to ensure the smooth flow of goods in and out of the EU

- provide authorities with shared, real-time data, enabling faster, more consistent and more effective risk management

- reduce administrative burdens for businesses and improve the accuracy of customs processes"

The EU Customs Data Hub is due to be operational on 1 July 2028, and by March 2034 it will handle all goods movements[3]. This rollout will be phased, and the plan is to give national authorities a complete overview of trade flows and supply chains, and access to real-time data across the EU to support much more effective risk management responses. The idea is that better data will lead to more accurate risk calculations – calculations of what cargoes to search

[3] EU Customs Reform, Latest developments (2026), https://www.consilium.europa.eu/en/policies/modernising-the-eu-customs-union, March, accessed 29 June 2026.

and where to use limited customs resources. The aim is to share data from many different data sources to get many different 'data perspectives' and enhance data quality using customs and border management data sources and other data sources from across the EU.

This aim supports the "*Smarter approach to customs checks*" pillar of EU Customs Reform which seeks to "*give customs authorities a bird's-eye view of the supply chains and production processes of goods entering the EU*" with access to real-time data and the ability to share risks information[4].

Clearly, data used in risk management decisions by customs organisations should not be completely open by default but the notion of making it open to appropriate entities like customs organisations is echoed in the EU's general stance on data reuse and data interoperability. For example, the EU Data Governance Act which provides a framework to "*enhance trust in voluntary data sharing for the benefit of businesses and citizens*"[5]. Also, the Interoperable Europe Act[6] sets out to create a network of interconnected digital public administrations by strengthening cross-border collaboration to build the foundations of cross-border digital services. Guidance for this is set out in the European Interoperability Framework[7]. And the principle that government data should be easily reusable[8] is a key pillar of the EU Open Data Directive, which is supported by Article 6 of the Union Customs Code (UCC)[9].

These aims and principles are based on the sound idea of collecting data from many diverse sources. Different organisations can gather different data because of their different situations, capabilities, connections and histories. And any movements of goods, people, money or information across national borders produces huge amounts of data at every supply chain stage before and after crossing even a single border. There are many stages and each stage produces data of some sort that is directly or indirectly available to different organisations, some public, some commercial. These different types of data describe what happens in each stage including

[4] European Commission (2026) EU Customs Reform, Taxation and Customs Union, https://taxation-customs.ec.europa.eu/customs/eu-customs-reform_en, accessed 6 July 2026.

[5] European Commission (2026) Data Governance Act explained, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained#main-content, accessed 29 June 2026.

[6] "Interoperable Europe Act", Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union, https://eur-lex.europa.eu/eli/reg/2024/903/oj, accessed 29 June 2026.

[7] IOPEU (2017) The European Interoperability Framework in detail, Interoperable Europe (IOPEU) Monitoring Collection, https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/european-interoperability-framework-detail, accessed 6 July 2026.

[8] "Open Data Directive", Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024, accessed 29 June 2026.

[9] European Commission (n.d.) The Union Customs Code (UCC) – Introduction, https://taxation-customs.ec.europa.eu/union-customs-code-ucc-introduction_en, accessed 6 July 2026.

any illegal actions. So, sharing data provides a more complete picture of whatever activities a cooperating organisation is tasked with managing.

The goal is not data sharing in itself but *interoperability*. But interoperability requires data sharing because shared data supports the decisions that enable coordination within and between organisations, including non-customs organisations. Decisions about what actions to take and what resources to use at the strategic and operational levels. Interoperability is crucial for customs organisations because only networks can fight criminal networks, and because the fundamental nature of supply chains and of cross-border movement, which are always networked, multi-stage and multi-stakeholder endeavours. This is true for criminals as well as non-criminals. Faking data trails at a whole journey level is nearly impossible because a huge number of data records all need to agree.

And there is an additional reason to promote more appropriate date sharing that has become much more urgent in the last few years. The new AI and Machine Learning (ML) tools that customs need for them to deal with the increasing volumes of global trade and the rising expectations of good manufacturers and their consumers, depend on high quality data[10]. Not just for initially training the AI and ML models that power these tools but also for enabling the decisions that these tools support when they are used.

But there is a major problem that limits the data that EU customs organisations and other appropriate organisations can share.

2.1. The problem with data sharing

The problem is that organisational attitudes to data sharing between customs organisations is highly fragmented and varied, and this limits data sharing. Even within the EU different histories, contexts, operational pressures and cultural drivers have led to different interpretations of the same EU laws. This in turn has led to customs organisations with different powers, mandates, organisational structures, border control practices, priorities, rules, methods and sanctions for non-compliance[11]. The recent report by the Wise Persons Group on the Reform of the EU Customs Union called it "*27 borders rather than one common border*", with data sharing at the "*whim of Member States*"[12]. Also, the European Court of Auditors notes that "*Member States do not systematically share information on risky importers with other Member*

[10] WCO (2025) Detailed report on the adoption of artificial intelligence and machine learning in customs, March, https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/smart-customs/public-version_detailed-report-on-the-adoption-of-ai-and-ml-in-customs.pdf, accessed 30 June 2026.

[11] European Court of Auditors (2021) Special Report 04 Customs controls: insufficient harmonisation hampers EU financial interests, https://www.eca.europa.eu/en/publications/SR21_04, accessed 30 June 2026.

[12] WPG (2022) Report by the Wise Persons Group (WPG) on the Reform of the EU Customs Union, Brussels, March, https://taxation-customs.ec.europa.eu/document/download/e5326383-2e8d-4d0e-9025-ddf262e9df6e_en, accessed 30 June 2026.

States", the EU's Customs Risk Management System (CRMS) is not capable of systematically sharing risk data and that "*each Member State only has information on those importers that it has itself assessed as risky*"[13]. These variations mean that criminals can avoid controls by changing the location where they clear imports to one where they are considered less risky.

2.2. The support for more data sharing, precedents and examples

There are many calls to enhance data sharing. For example, the World Customs Organisation (WCO) strongly encourages customs organisations to develop cooperative relationships and establish bilateral or regional agreements on customs cooperation or mutual assistance[14]. Indeed, Cooperation and Information Exchange is one of the seven key attributes of the WCO Risk Management Maturity Model. This encouragement covers central, regional and local levels of cooperation as well as external stakeholders in the private sector, and international cooperation between WCO and other international organizations, such as, Interpol, Europol, International Chamber of Commerce (ICC), International Air Transport Association (IATA) and the International Maritime Organisation (IMO).

The Wise Persons Group report on the Reform of the EU Customs calls for the current transaction-based and border-focused approach to be upgraded to a systems-based approach because "*Evidence gathered during the work of the Wise Persons Group shows that dangerous, non-compliant products still enter the EU market every day*". And "*the low level of data sharing across Customs administrations leads to fragmentation and makes it extremely difficult to properly manage risks through data analytics at both national and EU level*"[15].

The Financial Action Task Force (FATF), set up by the G7 to fight money laundering,

> *"… Egmont Group, INTERPOL and the United Nations Office on Drugs and Crime (UNODC), are calling for stronger global collaboration among analysts, investigators…"*[16].

Pillar 3 of the WCOs SAFE Framework of Standards deals with relationships between Customs and other government and inter-government agencies, and it states:

[13] European Court of Auditors (2021) Special Report 04 Customs controls: insufficient harmonisation hampers EU financial interests, https://www.eca.europa.eu/en/publications/SR21_04, accessed 30 June 2026.

[14] WCO (2023) Customs Risk Management Compendium Volume 1, https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/risk-management-and-intelligence/risk-management-compendium-volume-1.pdf?la=en, accessed 6 July 2026.

[15] WPG (2022) Report by the Wise Persons Group (WPG) on the Reform of the EU Customs Union, Brussels, March, https://taxation-customs.ec.europa.eu/document/download/e5326383-2e8d-4d0e-9025-ddf262e9df6e_en, accessed 30 June 2026.

[16] FAFT (2025) FATF, Egmont Group, INTERPOL and UNODC call for stronger co-operation between countries as they launch handbook to fight money laundering, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/international-cooperation-against-money-laundering.html, accessed 27 July 2026.

" Cooperation across various agencies is essential at the national level. Given the nature of the global supply chain, such effective cooperation must also be promoted bilaterally and multilaterally between and among organizations representing different sectors and regulatory areas in order to foster and establish international harmonization and reduce burden on both trade and governments."[17]

Veenstra and Heijmann in the World Customs Journal also recommend a systems-based approach for "*regulations that require enforcement based on information of the entire supply chain*" … "*not only supervision at the border, but also supervision at the product level or of business behaviour*". They point out that the operation of a whole supply chain cannot be authenticated just with a transaction at the border and help from other agencies from inside or outside the same customs territory will be frequently needed. Either additional capabilities need to be developed or co-operation with those authorities that have these capabilities must be secured[18].

A joint report by the World Trade Organization (WTO) and the WCO suggest that sharing of information amongst all relevant stakeholders in real time is a major benefit of introducing blockchain technologies and highlights the issue of the lack of trust in data sharing[19]. The risks of data sharing frequently combine with the theme of trust. For example, Canada's parliament highlighted that

"…misperceptions of legal risk and mistrust between agencies continue to hamper information sharing within the national security community."[20]

There is also strong support for large scale international data sharing, including EU Council Regulation and Directives to enable smoother international data sharing across the EU for value-added tax purposes[21] and direct taxation purposes[22].

[17] WCO (2025) SAFE Framework of Standards, June, https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/safe-package/safe-framework-2025_en.pdf?la=en, accessed 30 June 2026.

[18] Veenstra A and Heijmann F (2023) The Future Role of Customs, World Customs Journal, Vol. 17, Issue 2, https://www.worldcustomsjournal.org/article/88415-the-future-role-of-customs, accessed 30 June 2026.

[19] WTO and WCO (2022) The role of advanced technologies in cross-border trade: A customs perspective, https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/wco-wto-paper/role-of-advanced-tech_en.pdf, accessed 30 June 2026.

[20] Public Safety Canada (2023) Parliamentary Committee Notes: Challenges Associated With the Use of Intelligence as Evidence in Civil and Criminal Proceedings, Committee notes, Canadian Parliament, https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20231013/11-en.aspx, accessed 22 July 2026.

[21] Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax (recast).

[22] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC.

The implementation of the EU Single Window is planned for 2031 with the aim of submitting shipment information only once to a single electronic portal[23]. This will require a great deal of data sharing, but the Single Window is a layer over national single window environments rather than unified system. It does not include all types of data sharing, for example it does not provide "*a 360-degree overview of supply chains and the movement of goods*", that is why the EU Data Hub is being created[24]. It does not cover ship data, for example ship arrival, stay and departure reporting is handled by the separate European Maritime Single Window environment[25]. And it has its own data sharing barriers to overcome, such as aspects of the European legal framework to establish "*a parallel functioning of both paper and electronic environments" rather than a fully digital one*[26]. Navigating complicated legal barriers is a part of any Single Window implementation, not just in the EU[27]. For an overview see the UNECE white paper on Data Governance For Trade Facilitation[28].

The WCO Data Model is a part-solution for technical data sharing barriers; it is a standardised "*universal language for cross-border data exchange*" which Single Window systems need to enable them to communicate with each other[29]. The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) develops similar standards[30].

Council Directive (EU) 2018/822 of 25 May 2018 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements.

[23] European Commission (n.d.) The EU Single Window Environment for Customs, https://taxation-customs.ec.europa.eu/customs/customs-controls/eu-single-window-environment-customs_en, accessed 1 July 2026.

[24] European Commission (2026) EU Customs Reform, https://taxation-customs.ec.europa.eu/customs/eu-customs-reform_en, accessed 1 July 2026.

[25] European Commission (n.d.) European Maritime Single Window environment, https://transport.ec.europa.eu/transport-modes/maritime/eu-wide-digital-maritime-system-and-services/european-maritime-single-window-environment_en, accessed 1 July 2026.

[26] Antov, M Peycheva B, Kostova S, & Zhelev Z (2026) Digital Aspects of Customs Control in the New European Customs Reform Initiative, *World Customs Journal*, *20*(1), 44–66, https://doi.org/10.55596/001c.156039, accessed 1 July 2026.

[27] ESCAP/UNECE (2012) Electronic Single Window Legal Issues: A Capacity-Building Guide, United Nations, https://repository.unescap.org/server/api/core/bitstreams/ed153d5e-6779-4075-8641-0d0d5860d11b/content, accessed 1 July 2026.

[28] UNECE (2024) Data Governance For Trade Facilitation, https://unece.org/sites/default/files/2024-11/WhitePaper-DataGovernanceTradeFacilitation.pdf, accessed 27 July 2026.

[29] WCO (n.d.) The WCO Data Model, https://www.wcoomd.org/DataModel, accessed 1 July 2026.

[30] UN/CEFACT (n.d.) Trade Facilitation and E-business (UN/CEFACT), UNECE, https://unece.org/trade/uncefact, accessed 1 July 2026.

Other data sharing networks include the WCO's 12 Regional Intelligence Liaison Offices (RILOs)[31]. National customs organisations can apply to join their local office and second staff to it[32]. The RILOs are a global network for data sharing, coordination and interoperability.

The recently formed Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) is developing the FIU.net system for EU Financial Intelligence Units and Europol to use to exchange information[33]. Financial Intelligence Units (FIUs) are national nodes for sharing financial information on topics including suspicious transactions, money laundering and terrorist financing. The network of 182 FIUs is overseen by the Egmont Group[34].

Sending mail internationally requires interoperability between national postal authorities and other organisations, and the Universal Postal Union provides detailed guidelines on exchanging data between customs organisations and national postal authorities[35]. The UPU's Multilateral Data Sharing Agreement (MDSA) supports the complicated multilateral data sharing agreements that are necessary for operating internationally[36]. The Prüm data-sharing framework agreed in 2005, and recently updated to Prüm II[37], enables law enforcement authorities in Europe to automatically crossmatch and exchange data to fight cross-border crime, terrorism, and illegal migration[38].

There are many technical precedents for data sharing – solutions to technical problem of connecting data sources and data requestors. These include the EU's Once-Only Technical System (OOTS) which is a secure infrastructure for government-to-government data exchange[39].

---

[31] WCO (n.d.) Regional Intelligence Liaison Offices, World Customs Organisation (RILO), https://www.wcoomd.org/en/topics/enforcement-and-compliance/activities-and-programmes/intelligence-and-risk-management-programme/rilo.aspx, accessed 1 July 2026.

[32] RILO (n.d.) RILO A unique and united network, WCO, https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/tools-and-instruments/rilo/rilo-brochure_en.pdf?db=web, accessed 1 July 2026.

[33] AMLA (n.d.) https://www.amla.europa.eu/faqs_en#role-and-functions, accessed 30 June 2026.
EU Financial Intelligence Units' Platform, https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&do=groupDetail.groupDetail&groupID=3251, accessed 30 June 2026.

[34] The Egmont Group (2026) About The Egmont Group, https://egmontgroup.org/about/, accessed 16 July 2026.

[35] UPU (2025) WCO–UPU Guidelines on the Exchange of Electronic Advance Data (EAD) and Data Quality, https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/customs/wcoPublicationsAndActivities/WcoUpuGuidelinesEadAndDataQuality2025En.pdf, accessed 6 July 2026.

[36] UPU (2021) UPU Multilateral Data Sharing Agreement (MDSA) – FAQs, https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/SupplyChainIntegration/mdsa/faqsMdsa_EN.pdf, accessed 30 June 2026.

[37] European Parliament (2026) Regulation on automated data exchange for police cooperation (Prüm II), Legislative Train Schedule, https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-pr%C3%BCm-ii, accessed 1 July 2026.

[38] EUR-Lex (2008) Stepping up cross-border cooperation – the Prüm decision, https://eur-lex.europa.eu/EN/legal-content/summary/stepping-up-cross-border-cooperation-the-pr-m-decision.html, accessed 1 July 2026.

[39] OOTS (n.d.) About OOTS, European Commission, https://ec.europa.eu/digital-building-blocks/sites/spaces/OOTS/pages/610468075/About+OOTS, accessed 1 July 2026.

The Electronic Exchange of Social Security Information (EESSI) is a decentralised IT system for sharing social security information between relevant organisations across Europe[40] and criminal records can be checked using ECRIS[41]. The Internal Market Information System (IMI) supports data sharing related to implementing EU law including one-to-one requests, one-to-many notifications and alerts, and a centralised database[42].

The EU's Common information sharing environment (CISE) supports data sharing between EU maritime authorities, civil and military, and across borders and industrial sectors[43]. Its purpose is to fight to threats at sea, including physical and cyber-attacks, critical infrastructure attacks, illegal migration, drug trafficking, and other crimes. It connects European and national maritime surveillance systems and includes a "Responsibility to Share" principle (RTS) which encourages CISE members to actively share information with other CISE Network members[44]. The CEN Suite is a set of law enforcement tools developed by the WCO Customs Enforcement Network (CEN) which includes a national database and a secure communication platform to support collaborate cross-agency collaboration[45]. Like CISE these technical solutions and depend on the willingness of national users to share and are very specific about what data they might share and whom they will share it with. This includes national as well as international-level data sharing.

Some networks offer human capabilities as well as mostly technical capabilities, and some are international-level networks that connect national-level networks. These include the Schengen Information System (SIS) which is a network for sharing alerts about people of interest with other countries that use SIS in real time[46]. The SIS is an IT system, so it depends on member countries setting up their own offices, called "SIRENE Bureaux", of staff with the appropriate expertise to access and use the system[47]. The Customs Eastern and South-Eastern Land Border

[40] EESSI (n.d.) Electronic Exchange of Social Security Information (EESSI), European Commission, https://employment-social-affairs.ec.europa.eu/policies-and-activities/moving-working-europe/eu-social-security-coordination/digitalisation-social-security-coordination/electronic-exchange-social-security-information-eessi_en, accessed 1 July 2026.

[41] ECRIS (xxx) Home page, European Criminal Records Information Services (ECRIS), https://ecris.eu/, accessed 10 July 2026.

[42] IMI (n.d.) About IMI, European Commission, https://ec.europa.eu/internal_market/imi-net/about/index_en.htm, accessed 1 July 2026.

[43] CISE (n.d.) Common information sharing environment (CISE), European Commission, https://oceans-and-fisheries.ec.europa.eu/maritime-security/common-information-sharing-environment-cise_en, accessed 1 July 2026.

[44] EMSA (n.d.) What is the Responsibility to Share principle and how does it apply to CISE?, European Maritime Safety Agency (EMSA), https://emsa.europa.eu/cise/faq-cise/item/3934-what-is-the-responsibility-to-share-principle-and-how-does-it-apply-to-cise.html, accessed 1 July 2026.

[45] CEN (n.d.) CEN Suite, WCO, https://www.wcoomd.org/en/topics/enforcement-and-compliance/instruments-and-tools/cen-suite.aspx, accessed 1 July 2026.

[46] SIS (2023) What is SIS and how does it work?, European Commission, https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system/what-sis-and-how-does-it-work_en, accessed 1 July 2026.

[47] SIRENE (2025) SIRENE cooperation, European Commission, https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system/sirene-cooperation_en, accessed 1 July 2026.

Expert Team (CELBET) was set up by 11 EU Member States (Finland, Estonia, Latvia, Lithuania, Poland, Hungary, Slovakia, Croatia, Romania, Bulgaria and Greece), under DG TAXUD supervision, to improve interoperability with more data sharing and new ways of joint working[48]. Other data exchange systems also depend on trusted contact points like the European CAR and driving licence Information System (EUCARIS)[49] where vehicle and driving-licence registration authorities act as national hubs and the ASEAN Single Window which connects national single windows into a network of national gateways[50].

Support for better data sharing, and the interoperability it enables, also occurs outside the EU, outside of government and within single countries. For example, the UK's the Data Sharing Network of Experts (DSNE) is a cross-government virtual team that was set up in 2022 to solve problems with sharing data between departments and agencies[51]. The International Data Spaces Association (IDSA) builds standards for safe data sharing in more than 30 countries[52]. Catena-X is a decentralised and secure data sharing network for automotive supply chain members[53]. The Gaia-X European Association for Data and Cloud AISBL (Gaia-X) is a European-led non-profit association for decentralised data sharing between many different types of organisations[54].

"*The Governments of Estonia and Finland are exchanging data across borders in an X-Road* Trust Federation"[55]

And X-Road is used in many other countries for secure data exchange between government and other organisations[56]. There are many more information sharing and data exchanges of different types that share information across borders including the EU's e-CODEX (e-Justice Communication via Online Data Exchange)[57], which is managed by eu-LISA along with several

[48] WPG (2022) Report by the Wise Persons Group (WPG) on the Reform of the EU Customs Union, Brussels, March, https://taxation-customs.ec.europa.eu/document/download/e5326383-2e8d-4d0e-9025-ddf262e9df6e_en, accessed 30 June 2026.

[49] EUCARIS (n.d.) homepage, https://www.eucaris.net/, accessed 1 July 2026.

[50] ASEAN (2026) Overview of The Sector, https://asean.org/our-communities/economic-community/asean-single-window/, accessed 1 July 2026.

[51] Soncul M (2025) Unlocking data sharing across government, UK Government Data Service, https://dataingovernment.blog.gov.uk/2025/04/07/unlocking-data-sharing-across-government, accessed 1 July 2026.

[52] IDSA (2025) International Data Spaces Global standards for trusted data sharing, International Data Spaces Association, https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Brochure-Global-Standards-for-Trusted-Data-Sharing_Oct-25.pdf, accessed 6 July 2026.

[53] Catena-X (2026) About us, https://catena-x.net/about-us/, accessed 6 July 2026.

[54] Gaia-X (2023) About Gaia-X, https://gaia-x.eu/about/, accessed 6 July 2026.

[55] OPSI (2021) X-Road Trust Federation for Cross-border Data Exchange, OECD Observatory of Public Sector Innovation (OPSI), https://oecd-opsi.org/innovations/x-road-trust-federation-for-cross-border-data-exchange, accessed 7 July 2026.

[56] X-Road (n.d.) X-Road World Map, https://x-road.global/xroad-world-map, accessed 7 July 2026.

[57] eu-LISA (2026) e-CODEX, eu-LISA , https://www.eulisa.europa.eu/activities/large-scale-it-systems/e-codex, accessed 7 July 2026.

other large-scale information systems[58]. Inside Europe, other networks include the Import Control System 2 (ICS2)[59], FIU.net which enables data sharing to fight financial crime[60] and many other IT systems that enable separate countries to function at the level of the whole "EU system". Outside Europe other systems, networks and methods to support data sharing enable interoperations that let individual, national or organisational elements combine their operations into a higher emergent level. These include Interpol's databases[61], INDIRA (customs records data between Mercosur members)[62], Singapore's Trusted Data Sharing Framework[63], New Zealand's Approved Information Sharing Agreements (AISAs)[64] and many others.

In summary, there is huge support for more data sharing and many precedents but data sharing between organisations remains highly fragmented and underused. Next, we describe our analysis of this tension between the pressure to share more and the barriers against sharing to try to look for a solution.

3. Data sources used in this research

We collected data from March 2024 to July 2026. During this period, we held semi-structured interviews, workshops and meetings with interviews with Dutch Customs, UK HMRC, Hungarian Customs, Canadian BSA, Irish Revenue, Bahrain customs, Norwegian customs, and New Zealand Customs. We informally discussed the theme of data sharing with customs staff and technology company staff at the WCO Technology Conference in January 2026. And we discussed the barriers to data sharing with customs-related attendees and organisers at the CERIS workshop on Innovative approaches to combating the trafficking of goods, in April 2026.

Documentary sources are provided in the footnotes.

[58] eu-LISA (2026) Large-Scale IT Systems, eu-LISA, https://www.eulisa.europa.eu/activities/large-scale-it-systems, accessed 7 July 2026.

[59] DG TAXUD (n.d.) Import Control System 2 (ICS2), European Commission, https://taxation-customs.ec.europa.eu/customs/customs-security/import-control-system-2_en, accessed 7 July 2026.

[60] EC (2025) 'Next-Generation' FIU.net, European Commission, https://finance.ec.europa.eu/news/next-generation-fiunet-2025-02-04_en, accessed 7 July 2026.

[61] Interpol (2026), Databases, Interpol, https://www.interpol.int/en/How-we-work/Databases, accessed 7 July 2026.

[62] CBPT (2024), Project, Cross-Border Paperless Trade Database, https://www.digitalizetrade.org/projects/information-exchange-customs-records-indira-system, accessed 7 July 2026.

[63] IMDA (2026) About the Trusted Data Sharing Framework, IMDA, https://www.imda.gov.sg/how-we-can-help/data-innovation/trusted-data-sharing-framework, accessed 7 July 2026.

[64] OPC (2013), Approved Information Sharing Agreements (AISAs), Office of the Privacy Commissioner (OPC), https://www.privacy.org.nz/about-us/information-sharing/approved-information-sharing-agreements, accessed 7 July 2026.

4. 4. Strategic Alignment with the EUCA Mission – Why Customs needs more data sharing

Many sources inside and outside the customs community strongly support more data sharing but there are also three additional reasons based on the logic of how the international customs system functions, the decisions and actions that customs analysis must make in the future and what is required to use the new AI technologies that will support them.

4.1. Reason 1: Interoperability and how a system function

Some form of information sharing between system elements is a fundamental requirement for the existence of that system. If anything is to be described as a whole entity rather than a collection of separate parts, the parts must communicate by sharing information about what concerns them, and the more they communicate then the more integrated their operations are at the system level. This includes the EU itself and any of network of border management organisations like the EU Customs Authority (EUCA)**.** Information sharing of all types constitutes to the way that the parts emerge bottom-up to create the level of the system. Without this there is no international customs system, the more information sharing on any subject is limited then the more the system fails to function in different ways.

4.2. Reason 2: New data enables new decisions and new actions

Information systems, which include hardware, software and people, take raw data and filter it into useful information, which combines into knowledge patterns. These patterns are useful if they show us options for action to choose from and help us to choose. This is how raw data is turned into information and then used to support decision-making and acting65. In border management, raw data is anything that might describe the goods, people, money or information that we are interested in. Information is hopefully within that raw data and can form a useful pattern. Patterns tell us potential options for action that give the likely best outcomes, and the actions are how to use limited resources in risk-based operational decisions.

[65] Shaw DR (2022) Managing Emerging Data Technologies: Theory and Practice, Sage Publications, December.

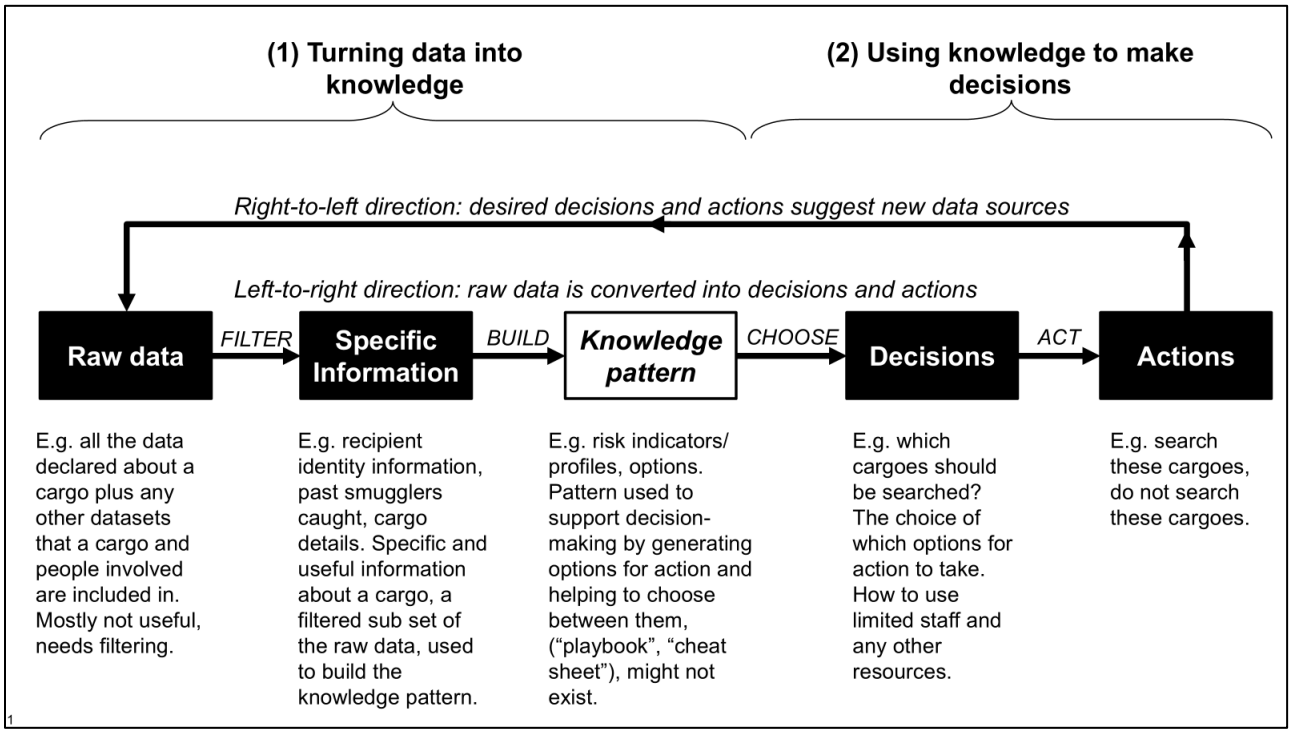


Figure 1 shows how raw data is used to make decisions in the left-to-right direction but the link between data sources and data, and decisions and actions, works both ways. This link can also be used in reverse in right-to-left direction. We can use potentially useful new decision-making technologies and the potential actions that might help an analysis to suggest new types of data and new data sources. For example, new AI and machine learning technologies give customs analysts the capabilities to analyse more data types, like video, more mixtures of data types ("multi modal data"), and higher volumes of data.

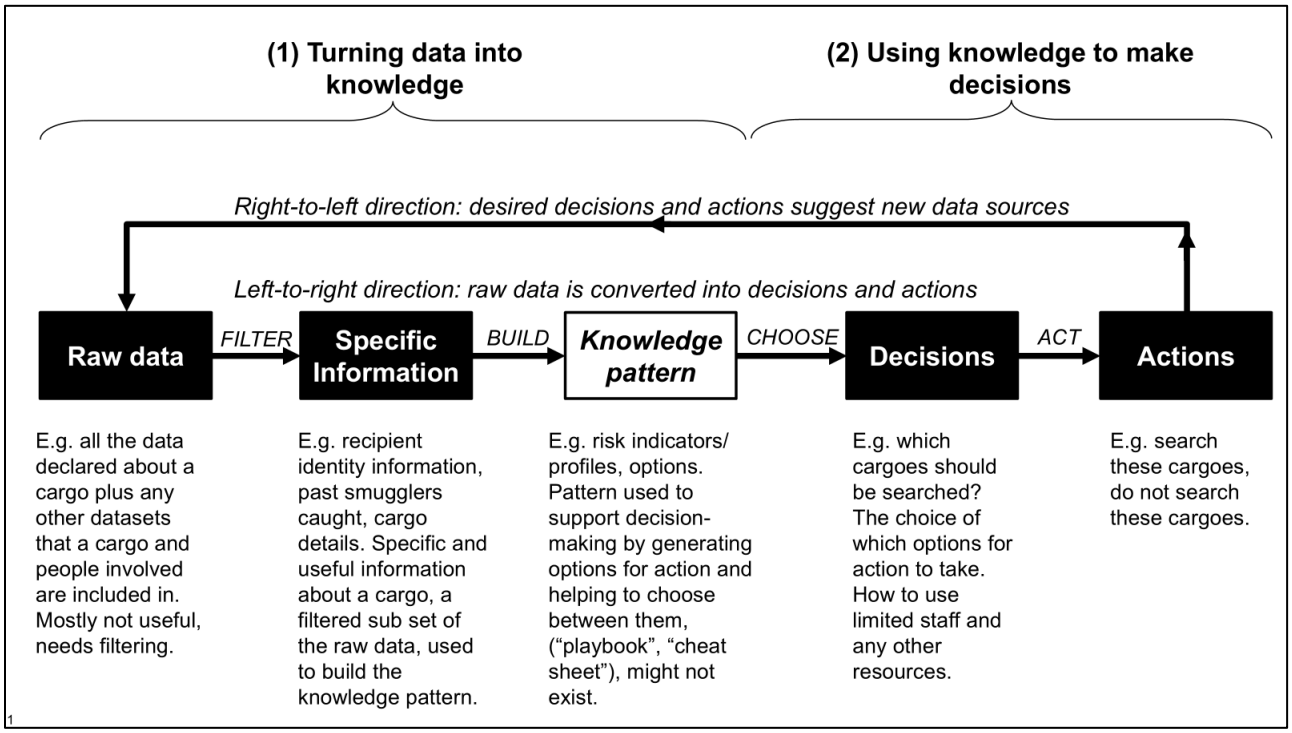


Figure 1: The Big Data Information Value Chain: How data, information, knowledge, decisions and actions relate to each other. Note how the right-to-left direction arrows represent ways of suggesting new data sources and data types based on new ways of decision-making, new decisions and alternative actions[66].

Data sharing is critical for risk-based operational decisions in border management because the goods, people, money or information that is being moved across borders each have individual physical journeys and more complicated 'information journeys' that are impossible to observe by any single organisation. Data sharing enables customs to get enough of the right data to find patterns in these physical and information journeys. Information journeys are the data trails that physical journeys produce in the many information systems that support, permit, monitor or just record each physical journey stage. These include logistics, transport, financial, commercial, government and other information systems. Figure 2 shows how physical journeys and information journeys have past, present and future aspects. Past aspects are past stages, the current aspect is the stage the traveller is at now and future aspects are the declared, likely or expected future stages. Past, present and future aspects that are declared by the person or entity responsible for a journey might be accurate, inaccurate or faked to different degrees.

[66] Based on the Big Data Information Value Chain model, Abbasi A, Sarker S, and Chiang, RHL (2016) Big Data Research in Information Systems: Toward an Inclusive Research Agenda, *Journal of the Association for Information Systems*, 17(2).

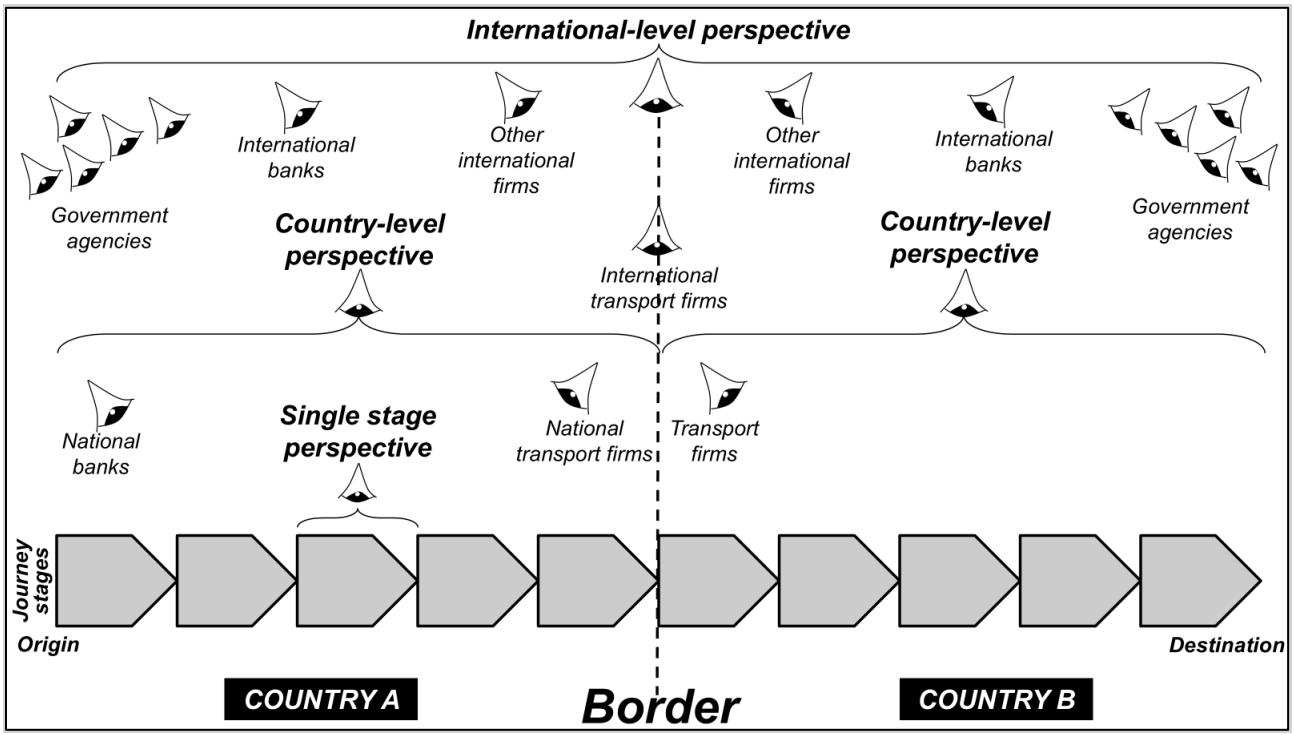


Figure 2: Physical journeys are made up of many stages, and each stage produces a data trail on an "information journey". Data trails are enabled and recorded by the information systems operated by different organisations, which gives them very different data perspectives on these physical journeys and the data trails that they generate.

Organisations record different data because their normal business operations are different; they have different products, services, business models and operational methods. They do different things for different purposes in different places at different times, all of which give then different "data perspectives". Data sharing between a mixture of organisations provides a much richer collection of raw data to analyse, which makes it more likely that customs analysts will find useful patterns.

Figure 3 shows some of the different types of data and data trails that various organisations have access to that record the same journey. You can see how data trails are generated by vehicles, people cargoes and other physical entities that are making the journey. Other data trails are made from the passive recordings of broadcasts made by travellers and their devices, some of which are directly involved in the physical journeys, and some are third party buyers and resellers of this data[67].

[67] Cyphers B (2022) Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police, EFF blogpost, https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police, accessed 22 July 2026.

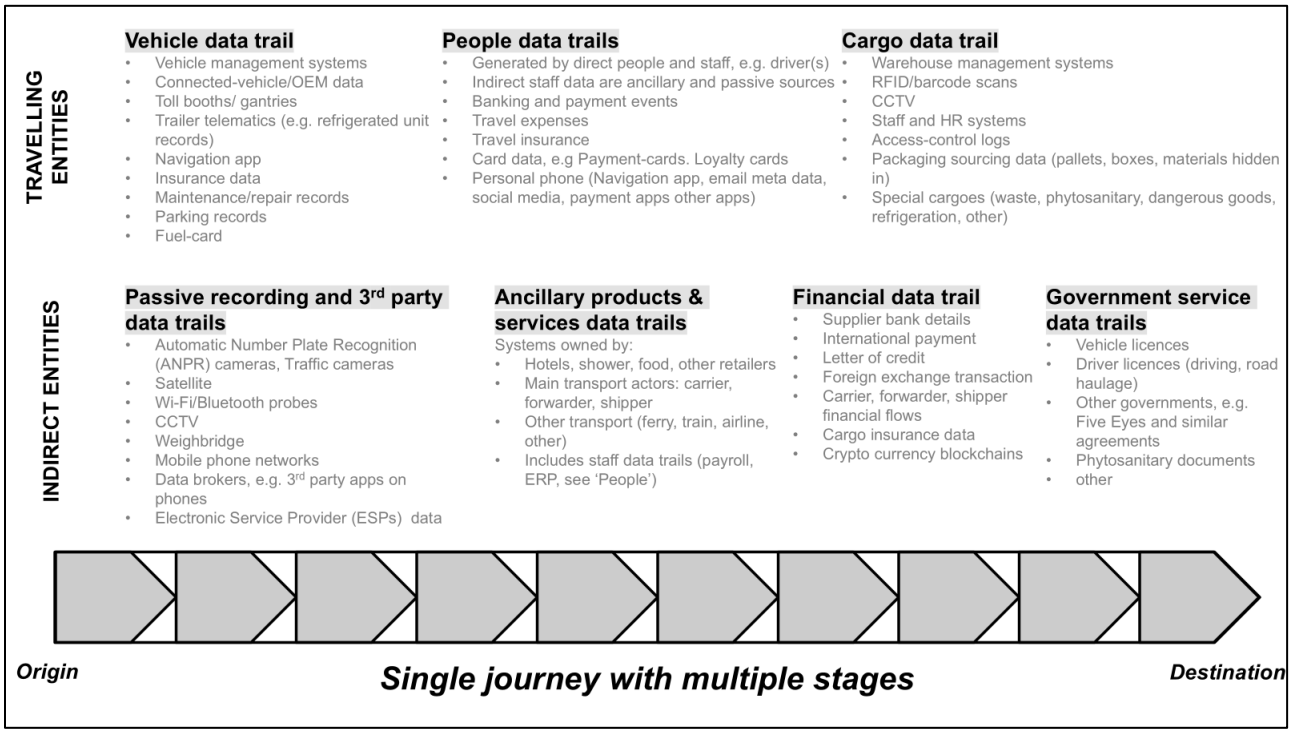


Figure 3: An entity's journey generates a bundle of overlapping data trails: the vehicle trail, the trailer trail, the driver trail, the cargo trail, the pallet trail and other entities. In each stage data is generated and recorded by the organisational IT systems that enable the travel.

Remember that 'travellers' means vehicles, people, cargoes and other physical entities. The data trails of ancillary products and services are the most complex type of data trail because they are made and recorded as part of the normal operations any organisations that enable a journey. Not just data trails recorded by hotels and food retailers, or ferries and trains, but any data trails of operational resources that do not travel on the journey themselves, but which support a journey stage. These include organisational IT systems like staff payroll records. Ancillary IT systems include those operated by all Electronic Service Providers (ESPs) which provide communications, digital transactions or data services (payment processors like Stripe and PayPal, or trust service providers like DocuSign and Adobe Sign, or internet service providers. In some countries ESPs are legally required to provide "*lawful access*" to data for law enforcement agencies[68]. The data trails of ancillary products and services theoretically go on forever in an expanding set of ripples that are generated at every journey stage. This makes

Fog Revealed: A Guided Tour of How Cops Can Browse Your Location Data, EFF blogpost, https://www.eff.org/deeplinks/2022/08/fog-revealed-guided-tour-how-cops-can-browse-your-location-data, accessed 22 July 2026.

[68] Canadian Government (2026) Lawful access, https://www.canada.ca/en/services/policing/police/crime-and-crime-prevention/lawful-access.html, accessed 22 July 2026.

them complicated to envisage but potentially extremely valuable because this same complicatedness makes them harder for criminals and terrorists to fake.

Another valuable group of data trails are financial, these include financial agreements, documents and records in banks and insurance organisations that are required for international shipments. For those wishing to hide data trails, it is almost impossible to not leave some form of financial trail. Even though crypto currency blockchains are seen by criminals to hide their identity and activities.

Finally, in a similar but less extensive way to ancillary products and services there are the data trails of the government services that are required for cross-border and in-country travel, for example licences, permits, certificates, authorisations and approvals.

By default, data trails data is created on separate IT systems, it is not usually created as a single linked up trail that spans many stages in a journey. Data is only linked together to make a data trail after data sharing. So there needs to be some way of linking individual shared datasets from the multiple IT systems that are in separate stages on the same traveller's journey. Most data trails do not exist until data is shared and linked together for some purpose such as a customs analysis of a journey. The problem of linking datasets together is similar how commercial retail organisations try to understand if the customer that visited the shop on Monday was the same person that visited the shop on Wednesday. Or if a customer that searched for advice on feeding babies is the same person that is looking at baby clothes on the website now. Linking datasets is needed to build up a picture of individual customers' behaviours so they can be treated individually, in the case of retail 'treated individually' means targeted adverts and personalised buying incentives. The problem is How to link pieces of data from different occasions and from separate sources? Retailers solve the linking problem by adding cookies to their phone and laptop browsers and persuading customers to join loyalty programmes, both solutions link together events in separate journey stages to construct a common data trail for that individual. In customs risk management this means checking the total journeys of cargoes, vehicles, people information and other entities to see if they are either as they were declared, or that they are not suspicious. Even when trails are faked, there are always previous and subsequent stage data, or direct and indirect supply chain data to be compared to find inconsistencies.

Combining data from different sources also enables the quality of any declared data to be checked. For example, is the declared cargo route consistent with past stage location data from organisations that helped the cargo to travel? Combining data also enables future behavioural expectations to be checked. For example, did a cargo go on to a next stage as expected? Next stages generate checkable data like a location, a dwell time or some other likely behaviour.

4.3. Reason 3: New AI technologies require more data sharing

There are huge opportunities in customs to use new AI and machine learning technologies, like Generative AI[69,70]. In Figure 1, the backwards, right-to-left connection between decisions and actions, and the data types and data sources used suggests how these new AI capabilities could be used. AI and machine learning technologies enable customs staff to use a much greater range of data types – 'multi-modal data' – and a much greater volume of data. This will apply even for ad hoc analyses much more than it does for standard and routine analyses. For example, the combination of digital computing speed and natural language instructions means that AI video search tools enable customs officers to quickly look through hours of video data using simple search prompts, like "look for two men handing a bag to each other" or "look for the same person who changed their appearance or who has changed clothes" or "which vehicles have been painted over or have driven past this spot the most today".

But if the potential of these technologies is to be fulfilled then they need to be fed with a much richer, more extensive and more varied set of data. In addition to video data this includes any type of ancillary data from the IT systems and sources in Figure 3, plus social network data and other open-source data from the World Wide Web.

Other AI capabilities point to more ways that AI can support customs analysis with decisions and these in turn suggest new the data types that will be useful for that. For example, natural language prompts make Generative AI tools more accessible and quicker to use, which means they are more practical for ad hoc analyses. Also, the Large Language Model (LLM) technology that enables Generative AI is naturally suited to finding complex links between vast volumes of diverse data types. That is part of its fundamental design. This combination of natural language prompts and finding complex links broadens the type of analyses that are practical from analysing objects to analysing behaviour.

> *"This is the holy grail of surveillance," said a European official whose country uses the technology on its cities. "We are able to look for behaviour, not objects — it has created a world of new possibilities."*[71]

Looking for behaviours rather than just objects creates the possibility a whole new class of data to analyse, which requires sharing from new data sources. Of course, there are frictional

[69] WPG (2022) Report by the Wise Persons Group (WPG) on the Reform of the EU Customs Union, Brussels, March, https://taxation-customs.ec.europa.eu/document/download/e5326383-2e8d-4d0e-9025-ddf262e9df6e_en, accessed 16 July 2026.

[70] WCO (2025) Detailed report on the adoption of artificial intelligence and machine learning in customs, March, https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/smart-customs/public-version_detailed-report-on-the-adoption-of-ai-and-ml-in-customs.pdf, accessed 16 July 2026.

[71] Srivastava M and Miller C (2026) New AI espionage powers trigger Putin camera scare, The Financial Times, https://www.ft.com/content/6f4d806c-eb22-4c32-8352-b82692d30e9f?syn-25a6b1a6=1, accessed 17 July 2026.

problems associated with implementing AI in organisations, including AI hallucinations, reengineering workflows to suite AI use and gaining the right context and experience to ask the right questions and judge the responses – this is the "human-in-the-loop" problem. But the more AI tools are used to support risk management decisions then the more data types and data sources will be demanded for those decisions.

Additionally, the quicker nature of using natural language and AI's extremely fast pattern searching makes it practical to do more ad hoc analyses – to do searches that are non-standard, non-routine, based on speculation, or that maybe have never been considered before. This is particularly important for developing new ways for customs to fight the novel techniques and practices that organised crime continually develop.

However**,** there are many operational barriers to the appropriate data sharing even though there are strong justifications and many calls for it.

5. Data sharing barriers

"…*the data needed for carrying out customs supervision, risk analysis and controls are fragmented and duplicated across multiple systems in a decentralised customs IT infrastructure*"[72]

5.1. Types of data sharing barriers

Table 1 lists different types of data sharing barriers from our research.

Barrier	Description
Technical Barriers	The data is technically impossible for an organisation to send, receive, store or to usefully analyse. E.g. the amount of data might be too big to store or transmit in a useful time. Or some data types might not be storable or transmissible. Or there might no common data language or the IT networks might be incompatible.
Organisational Priority	A sender organisation is not motivated to send a dataset because it is not a priority and sending the data consumes resources.
Organisational Purpose/ Mandate	Sending the data is not considered to be appropriate or not part of what the organisation is for.

[72] EC (2023) Executive Summary Of The Impact Assessment Report, Proposal for a Regulation of the European Parliament and of the Council, establishing the Union Customs Code and the European Union Customs Authority, and repealing Regulation (EU) No 952/2013, European Commission, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023SC0141, accessed 1 July 2026.

Legal/ Regulatory/ Security	Sending the dataset is against the laws or rules that the organisation works under. E.g. privacy laws or organisational procedures. Includes security rules that are based on caution not law.
Cultural Norms	Sending the dataset is against the norms of the organisation. E.g. cultures of secrecy, cultural distrust of a receiving organisation. Anecdotally, even when customs staff move to another agency, they are renowned for not sharing information gained in the old agency. And vice versa.
National Sovereignty/ Norms	National-level cultural norms based on historical relations between the sending and receiving country, distrust of receiving country.
Capacity	The sending organisation is willing and able to send the dataset but does not have the capacity to do it. E.g. Special legal or IT expertise, or repeated approvals for frequent data sharing.
Purpose of Data Capture	How or why the data was captured was too different or a barrier itself. E.g. private data to be used for purposes other than originally agreed, or data 'illegally' captured
Data Quality	Some characteristic of the dataset is not fit for the receiver's purpose in using it. E.g. specific content, focus, scope, granularity, timeliness and other data quality dimensions.
Method of Data Capture	The way the data was generated introduces bias or reduces data quality in some way.
Downstream Workflows and Consequences	There is a risk of invalidating or derailing subsequent workflow stages. E.g. when legal/ prosecution processes are derailed if evidence is not gathered appropriately. Or if sending data to another country would result in a sentence of execution.
Reputational Risk	Asking for the data or sending it shows an organisational capability weakness. E.g. asking for data shows you cannot get it yourself.
Operational Secrecy	Asking for data shows what the receiver organisation is interested in.
Authoriser Accountability	There is risk of sanction for agreeing to send the data. E.g. for however sent the data or formally gave permission. This is compounded by the hierarchical nature of customs organisations, which means that usually the risk is for one person. This in turn produces a competitive risk to a person's career and a personal legal risk for little or no

	personal gain. And usually, there is almost no punishment for no action (don't miss/never had).
Specificity Tension	The less specific the data request then the more difficult it is to share because more data is requested and more barriers are triggered. But the purpose of data sharing is to look for potential patterns or matches in a dataset, not known patterns. So, the larger the dataset then the higher the probability of a hit.
Language Used in the Data Request	The choice of phases used to request data generates an 'atmosphere' that can oppose or support sharing. E.g. phrases like 'your data' gives the impression of giving away owned assets for no return. But phrases like 'appropriate information' lead to feeling of more control and less risk.
Asymmetric Benefit	No direct or clear benefit to the sender organisation, or the people involved in sharing the data.
Other Bilateral Asymmetries	Barriers depend on direction of flow. Sharing from organisation A to organisation B might be much harder than B to A.
Loss of Control	The sender cannot control onward use of the data. E.g. use for other purpose, repeat use, onward sharing.
The 2-Level Trap	Leaders that are senior enough to authorise a data share may not have close enough visibility of the situation to fully understand or be aware of the need. Operational staff who understand the situation may not have the power to authorise that data share. Causes delays which may remove any benefits of sharing for the data requester. There may also be a capacity constraint that limits the maximum number of authorizations in a time period.
Ad Hoc Analyses	Ad hoc analyses are non-standard and non-routine customs analyses with customised characteristics that are not preauthorised and not well-practiced compared to routine analyses. They may include new data, new data sources or new uses of current data that are not covered by current authorisations. A common way to develop new analysis strategies. A symptom of the limited types of data used in customs analyses.
Timeliness	Delays getting some data required in an analysis make that analysis unfeasible.
Higher Frequency Analyses	As ad hoc analyses transition to routine practices their frequency rises at a rate that is constrained by some resource bottleneck. E.g. when getting high level

	authorisation to share data takes up too much of the authoriser's time.

Table 1: Different types of barriers to data sharing with examples. Datasets are collections of data of any type and size. Data senders and receivers are usually in separate organisations, but this is not always clear, e.g. when legal powers or access to capacities and capabilities vary across an organisation. Or when a single government is considered to be a collection of separate ministries and other separate agencies. Includes sender and reivers in the same country and part of the same government, as well as international data sharing.

5.2. Data sharing barriers are either 'blocks' or 'gaps'

Fundamentally, the barriers in Table 1 are either blocks or gaps. Blocks are active oppositions to sharing data, for example legal barriers, rules, cultural mistrust or low prioritisation of resources. Something that has been constructed or has developed to block data sharing purposefully or by accident.

Gaps are missing commonalities for data transfer caused by separations and differences between the data sender and data receiver, for example compatible IT systems, shared data definitions and dictionaries, permissions, mandates, or missing critical resources. The data sender and data receiver are in some way separate organisations, or there would be no need to share. Their separate individuality and history cause incompatible differences, gaps, so a common 'bridge' needs to be built. Clearly, many organisations have something in common, they might be both part of the EU or they might be both border management organisations with shared interests, but there still could be gaps that need a bridge – a common platform– to be constructed or no data can be shared. All the systems, networks, membership organisations, regular meetings and methods in section 2.2 are bridges to cross different types of separation barriers that divide data senders and data receivers. However blocks are directional, they can work in one or both directions, and gaps are bidirectional. Platforms are required to bridge gaps or remove blocks.

On one level there is a similarity between the prioritisation of resources that causes blocks and the complete absence of resources that causes gaps. They both imply a lack of *willingness* to use some resources directly to unblock, or to bridge a gap. Willingness is a reoccurring theme in our research into data sharing barriers. For example, data sharing might fail even though many of the IT systems for data transmission, storage or analysis are in place. Encrypted web-based systems like S-CIRCABC or federated systems like CISE and X-Road. But permissions, mandates and the *will* to give them needs to be gained and this means persuading groups of different people.

5.3. Data sharing is always bilateral and directional

The large number of combinations of data sharing barriers explains why data sharing is always bilateral and directional. The barriers are different for each sender and receiver duo, and also

different depending on which of the two is the sender of the data and which is the receiver. Combinations of data sharing barriers are asymmetrical, different in each direction. Sharing from country A to country B must deal with different barriers than sharing from B to A. Even multi-country data sharing agreements like Five Eyes and others[73] require all countries to be *individually* comfortable with which specific data they send to which specific countries. For example, some countries want to share data but are legally barred from data sharing that might cause executions of people in countries that use capital punishment. Sharing depends on who the sender is and who the receiver is.

The benefits of data sharing are also asymmetric because there is no benefit to country A if country B returns the data it received from country A. And different organisations and countries have different requirements for extra data from external sources because of their different data perspectives (see Figure 2). So, the benefits that justify a data share must be indirect. Either from future reciprocal data shares from B to A, or from data shared from country C to country A, because all three countries are part of reciprocal data sharing agreement, see Figure 4 panel (b). Bilateral asymmetry applies at the organisational level as well as at the country level, it is just that organisations in the same country or legal regime, like the EU, may have more in common and so less barriers between them.

Reciprocation is important because it shows why only networks can fight networks. These types of multi-organisational and international data sharing agreements are required to fight people smuggling supply chains crossing several countries, or criminal networks with a range of criminal activities that concern customs as well as other government organisations. Direct reciprocation relationships are less valuable that indirect reciprocation networks because there are more indirect sources to receive data from, so they hold a greater variety of data.

[73] UNSCR (2026) Five Eyes, Nine Eyes, Fourteen Eyes: Where Your Data Is Subject to Compulsion, blogpost, https://unscr.com/blog/five-eyes-nine-eyes-fourteen-eyes-jurisdiction/, accessed 22 July 2026.

Koch R (2018) What countries are in the 5 Eyes, 9 Eyes, and 14 Eyes agreements?, Proton blogpost, https://protonvpn.com/blog/5-eyes-global-surveillance,

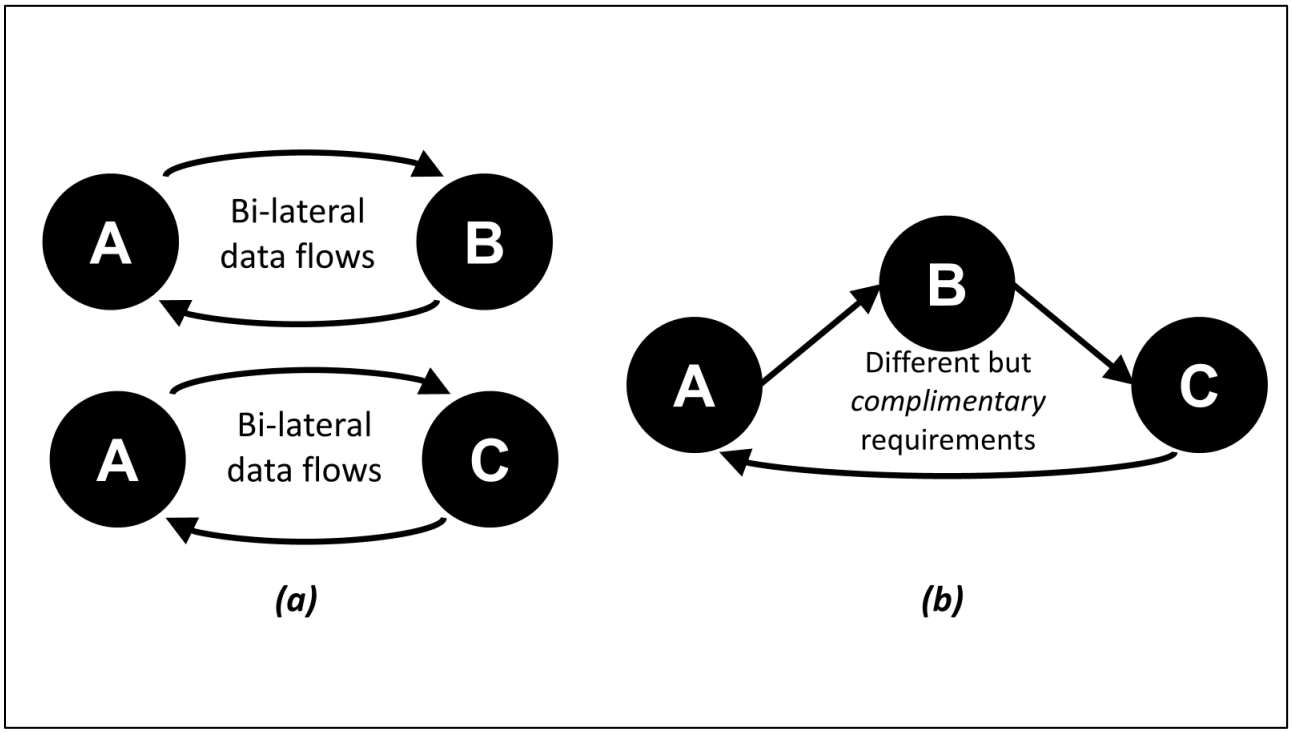


Figure 4: (a) Each bi-lateral share is different with different combinations of barriers and benefits, A to B ≠ A to C. Also, the barriers and benefits are different in each direction A to B ≠ B to A. (b) Indirect reciprocation is more likely to be beneficial than direct reciprocation because there are more sources to receive from, so there is a greater range of potentially valuable data. A and B have different data and data requirements but C's priorities 'complete the equation'.

5.4. Risky barrier combinations are the fundamental challenge

The data sharing barriers listed in Table 1 can occur individually but usually more than one of them occurs at the same time, which makes data sharing much harder. For example, the 2-level trap (where permission givers occupy a much more senior level than permission requesters) may combine with Ad hoc analyses (which need different data each time) and the Timeliness barrier (the maximum time for analysis to be useful) to make gaining authorisation or even getting the new data for an ad hoc analyse take too long. Or the process might take too much of the authoriser's time for the number of ad hoc analyses that the analyst needs. Ad hoc analyses are important because they are a way of developing and testing new standard analyses and improving customs practice. And as the varieties of data, data sources, data analysis technologies and criminal practices multiply the menu of standard analyses that are available to a customs analyst must also grow.

Other examples of confusing and overwhelming combinations of barriers include when Operational Secrecy makes it difficult to understand the Method of Data Capture and therefore the quality of the source's data. The Specificity barrier (where less specific data requests ask for

larger datasets) combine with barriers caused by the Language Used in the Data Request to make a data request seem riskier for the authoriser or the sender. Similar relations also affect perceived risk, like when Downstream Workflows and Consequences could potentially result in some of the other barriers being triggered. But it is frequently not clear which barriers might be triggered, why and what the risk is.

The risk of authorisation caused by confusing and overwhelming combinations of data sharing barriers is the central risk of risk management data sharing. And it produces the fundamental challenge for any customs staff who want to send data, request data or even authorise data to be shared with a separate organisation. The problem is that the effects of combinations of data sharing barriers are extremely hard to assess. They give the impression of being impossibly complex. A huge knot of interrelated problems that are too complex to even understand let alone solve. In this sense 'gives the impression of being impossible' is functionally the same as 'actually impossible'. When even describing the problem is too difficult it becomes impossible to solve it.

The different combinations of barriers, their interactions and the downstream effects that reach back to impact upstream staff members' authorisation decisions make data sharing risky for all those involved. Both in terms of judging consequences as well as the probability of those consequences. This is especially sensitive for customs staff who are operationally trained and culturally conditioned to protect their borders.

The bewildering combinations of many different data sharing barriers seem to make data sharing too risky for customs staff wanting to authorise, send to or request data from a separate organisation because they cannot easily judge the risk.

The risk of sanction for agreeing to share data is a huge barrier to authorisation. This is compounded by the hierarchical nature of customs organisations, which means that the risk is usually for a single person. It is a significant competitive risk the authoriser's career and a personal legal risk for little or no personal gain. Furthermore, usually, there is almost no punishment for inaction because no one misses data that they never had before – especially when the omission is experienced by a separate organisation.

It is ironic that risk is the biggest barrier to risk management, but we have found that this is *perceived* risk not actual risk.

6. Key findings: How to reduce the risk of risk management data sharing

6.1. Key Finding 1: The Data Trail Model – Visualising the big picture of direct and indirect data trails

The idea of data trails from the section 4.2 can be used in a Data Trail Model (DTM) to visualise the potentially useful data which might be available and the data sources to request it from. The DTM combines the idea that different organisations can record different data because they have different perspectives (in Figure 2), and as a cargo, a person or information travels through each stage of its journey it produces the different types of data in Figure 3. The DTM gives the 'big picture' of the bundle of overlapping data trails that are generated by an entity's travel. The DTM can be used to visualise what data is out there, external to the organisations that an analysis works in, so the analyst can decide which organisations to source data from. The first barrier to data sharing is knowing what is available. Modelling what might be available helps to think about who and where to get it from.

Additionally, the DTM's picture of whole-journeys and multiple data types helps in assessing the benefits of asking for data because it includes an understanding of the context of how that data was generated, which helps to describes the information and knowledge patterns that might be included in that data (Figure 1). It also shows a range of data trails, data types and sources to choose from. By considering the multiple journey stages and multiple data-trails the DTM helps information sharing requests to be more specific and therefore easier to agree to because the purpose of the required data is clearer. For example, the model forces analysts to specify the type of entity that is traveling, which in turn defines elements of the physical journey, which then makes it easier to define the associated informational journeys and the indirect entities that support both (Figure 3). Using the model like this helps an analyse go from the general to the specific using a chain of decisions about their analysis strategy.

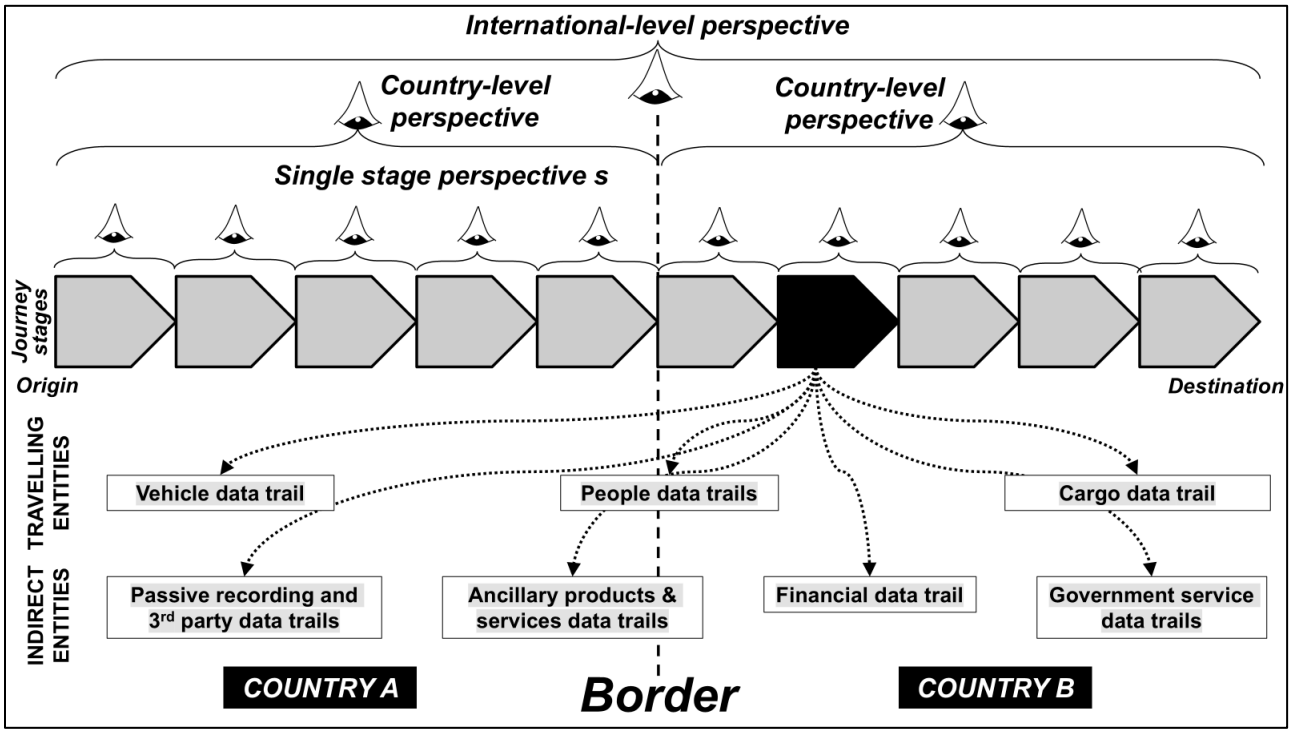


Figure 5: The Data Trail Model (DTM) helps analysis decide which data is required and where it might be sourced from because it combines journey stages and super stages, organisations that have different levels of perspectives and the data trails that different direct and indirect entities produce as journeys progress.

We don't recommend getting all the data that is laid out in a DTM, instead use the DTM as a map to decide exactly which data is required, what data is available and which sources to ask first. For example, in Figure 5, a vehicle moves through the black journey stage in country B and generates financial data trails associated with the vehicle and the people who operate it. But the ancillary services that these people and the vehicle consume, like food and fuel, also generate a cloud of data trails that can help to confirm the behaviour of the vehicle and its operators. Furthermore, the devices of the vehicle and its operators are recorded passively, for example using Wi-Fi or Bluetooth transmission, which can also confirm movements and other behaviours. But the staff and vehicles associated with the ancillary services also generate data that can be checked as part of providing their services.

6.2. Key Finding 2: The BADS model – Understanding data sharing relationships between organisations

These ideas suggest a method of thinking about data sharing relationships between many organisations, using each bilateral data sharing relationship as a building block. Focusing on each bilateral relationship one-by-one makes it much easier to assess the risks and benefits involved because they are defined by that relationship in each direction. And permutations are

limited to the bilateral level, so they do not scale with additional senders and receivers. Easier assessment of the risk of sharing data in turn lowers the *perceived* risks, and making the benefits more visible makes data sharing more attractive. Data sharing therefore becomes more likely.

Admittedly, data senders must consider whether a receiving organisation will pass the data on but considering that at the bilateral level is simpler than than considering the infinite permutations of passing data on, so it preserves the vast majority of data sharing opportunities.

The Bilateral Asymmetric Data Sharing Model (BADS) in Figure 6 provides a way of assessing the risk of sharing data by thinking about data sharing barriers bilaterally, which means considering the problem to be *complicated* rather than *complex*. There are many different barriers in each direction of a bilateral data sharing relationship, but they are not infinite and more importantly they do not all relate to each in complex ways. There are some combinations between sharing barriers, but every barrier does not depend on every other barrier to generate to many permutations that need assessing for risks before data is sent. Also, the asymmetry of each sharing relationship breaks the problem into two smaller problems, one for each sharing direction. Different potential data receivers present different problems for different senders. This bilateral and asymmetric view of data sharing barriers is illustrated in Figure 6 with steps on the left and right representing a data sharing network of organisations built out of many one-to-one relationships and different coloured circles representing the different data sharing barriers for each direction of sharing. Some of the barriers in each direction are different but many are the same.

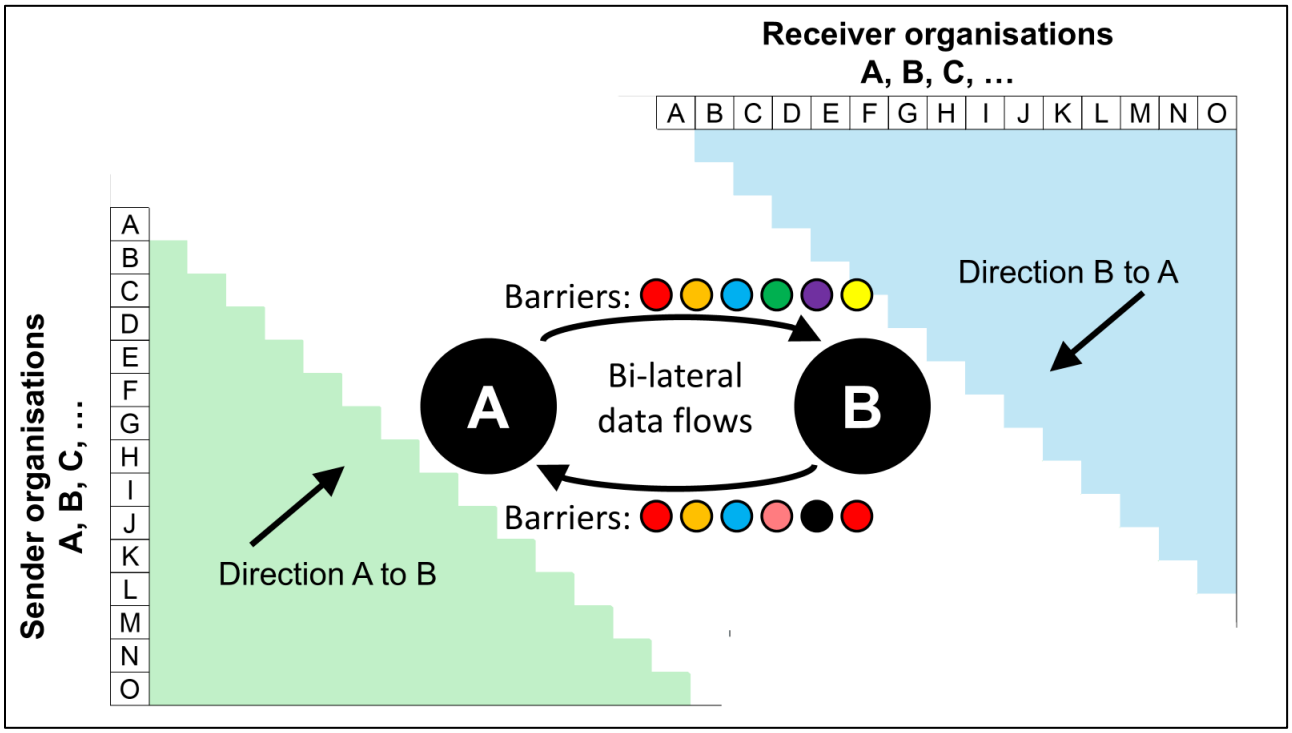


Figure 6: Combinations of barriers between data senders and receivers are complicated not complex. They only scale linearly with additional senders and receivers – risks can be assessed at each bilateral level rather than the level of a whole network of senders and receivers. There are a limited number of combinations of barriers, different in each direction, but with many in common.

6.3. Key Finding 3: Checksum-based data sourcing strategy – Kich-starting the data sharing journey

The DTM has an additional role, it enables analysts to think about the behaviours of the entities of interest rather than just their characteristics. What these entities do or don't do rather than just what they are, or how they appear. Behavioural data is important because people and vehicles are not illegal in themselves, sit's how they behave and how they are used that is important. People, vehicle and cargoes may appear to be completely legitimate until something about how they behave or how they are used is noticed from looking at the data trails they generate. Something odd, something that stands out. Something that does not fit normal behaviours for that type of entity. Or something that does not match expectations, or a likely progression of journey stages. This applies to direct and indirect entities.

The DTM is a method of thinking about data trails – which entities and behaviours generate them, how they are recorded and who might collect that data. As already mentioned, this is useful for planning an analysis strategy – deciding what decisions and data are required. But the additional value of the DTM is in helping analysis to pick which decisions and data facilitate

another type of journey, the journey of implementing a data sharing relationship between two organisations, the basic building block in a data sharing network.

The easiest way to start a data sharing relationship is to request very low sensitivity, abstract and anonymous data. Data that is easy for the sender organisation to think of as low risk and impersonal – a sort of 'data trail checksum'. A checksum is a small digital fingerprint which verifies that a data file has not been corrupted or altered during transmission or storage. It is a single number that is calculated using a sample of the data in the file to be checked. The checksum of the file is recalculated after transmission and if the new checksum does not match the old checksum, then the file has been corrupted. It works by distilling the essence of the whole file into a much smaller abstraction, a single number.

A data trail checksum is a small piece of relatively abstract data – maybe from an ancillary source –that confirms the existence of a much larger data trail. It does this by confirming behaviours that can only have been recorded as part of a journey route. The data trail checksum only gives a match if a data trail has been generated, only if some entity has travelled. Data trail checksums are not mathematical like file corruption checkers. They check expected behaviour using data that is not sensitive, and therefore easy to request and share, but which confirm that a person, vehicle or cargo did or did not do something. For example, data that proves a cargo cannot have travelled the route that had been declared, or that a person bought something or never bought anything from an organisation. By doing this data trail checksums justify greater data sharing.

Indirect data trails, especially those using ancillary sources, provide a valuable menu of data trail checksums because they are too plentiful to easily fake all of them, their indirectness might make their data less sensitive, and they are collected by a larger range of organisations. Some of which are commercial organisations which are accustomed to exchanging appropriate data to help them understand their customers better.

Data trail checksums can help to initiate and progress a data sharing relationship because they provide a low risk start and also, they map out a continuing pathway. The DTM helps because it connects direct and indirect entities, journey stages and super stages, past records and future expectations, organisational data perspectives, organisation data sources, supply chains levels of analysis and the data trails that are produced by all entities' behaviours as they travel. These connections provide a pathway from abstract low risk data to more useful data as trust grows, personal relationships develop, mutual understand arises and perceived risk reduces.

More work is required on choosing standard data trail checksums and their sources. Key questions include:

- Which data trails are hardest to fake or least likely to be fakes?
- Which data trail checksums are easiest to obtain from commercial or government organisations?
- Which is open-source data useful as a checksum? Which sources?

Three illegal movement scenarios suggest themselves as a way of further refining the different types of data trails. The scenarios are:

- "Do It Yourself" (DIY): the shipper is a private citizen, and movement uses a car, van or private vehicle. The scenario's distinction is that the shipper is private citizen. How does this distinction affect which data trails exist, and the data recorded on them?
- "Trojan Horse": the shipper is a legal organisation whose management know about the illegal actions and substitute an illegal cargo for a legal cargo, for example a scheduled deliver of drinks cans containing cocaine. There could be single or regular shipments. The scenario's distinction is that the management know. How does this distinction affect which data trails exists and the data recorded on them?
- "Cuckoo": the shipper is a legal organisation whose management *do not* know about the illegal substitution of an illegal cargo for a legal cargo, for example a scheduled deliver of drinks cans containing cocaine. There could be single or regular shipments. The scenario's distinction is that the management do not know. How does this distinction affect which data trails exists and the data recorded on them?

In these scenarios the distinctions point to potential data trails and stages on them that could confirm legality and justify further data sharing. These need to be discussed with users as part of the next steps.

Another way of choosing checksums from the DTM is based on whatever triggers the request to share data. Even if the detailed reasons for asking for some data are not themselves appropriate to share with the potential data source they may point to which data trails and which stages on them are of interest. A request for abstract and indirect data using the language of data trail checksums might hide the reasons for needing that data in a way that asking for data that is more directly connected to an entity of interest would not.

Furthermore, the criminal stakeholder system might be the trigger that initiates an ad hoc analysis. The criminal stakeholder system is the set of actors who take illegal actions which initiate the physical and informational journeys whose data trails we are we are concerned with. The three scenarios above have very different sets of stakeholders, who generate very different data trails that vary from their legitimate versions in distinctive ways. Criminal stakeholders produce very different data trails to non-criminal stakeholders.

These are more questions to be discussed with customs experts to reality-check these ideas and refine the methods they support.

7. Conclusions

There is a policy problem involved in implementing the EU Data HUB and the EU Customs Authority that also impedes the data sharing and interoperability aims of the BORDERLINK project. The problem is that the many combinations of data sharing barriers seem to make data sharing risks impossible to judge. Which hinders and delays authorisations.

The BORDERLINK project's deliverables around databases for cigarettes, Raman spectra and x-ray models are safe but the contextual data and other ad hoc data requests that are triggered by using these databases will be much more difficult to satisfy because they will be non-standard and non-routine. Innovations like these new BORDERLINK databases grow the core of customs practice, which triggers new ad hoc data analyses around the periphery. Ad hoc data analyses are required to keep up with new criminal practices, new data and new data analysis capabilities and they lead to new customs techniques and methods.

The solution to this problem is the insight that all data sharing, even when involving many organisations, can be thought as a collection of bilateral sharing relationships. And whilst the barriers for each bilateral direction are different, there are common types that do not interrelate. There is not an infinite number of barrier permutations just a relatively small list of common barriers that can be analysed and solved for each sender and receiver pair.

Furthermore, the data that is requested and potentially shared can be assessed in terms of the data trails it forms part of and the behaviours of the entities that generate it using Data Trail Models (DTMs). DTMs provide a 'big picture' and a context to choose from. They help with requesting less sensitive as well as more useful data because they connect data types with how that data is generated and why, and they apply to both the indirect as well as the direct traveling entities that cause the data.

Additionally, the 'big picture' of a DTM helps analysts to find 'data trail checksums', which are small, low sensitivity and probably indirect data for confirming the existence of certain data trails that in turn confirm the behaviours of the entity being analysed. Data trail checksums' can potentially be used to confirm ideas about criminal behaviours that justify more extensive data sharing.

Finally, as part of the validation phase of preparing this policy paper we have discussed our findings with senior customs experts including different solutions to component bilateral sharing barriers such as *mutualised authorisations* of data shares to share authorisation risk. We will test the logic and extend this and other methods mentioned here in a discussion process that seeks to raise awareness of these barriers and solutions, to form consensus and to potentially support the design of the EUCA. As such we hope to engage with those involved in

planning the Risk Management Operations of the EUCA even though they have not been recruited at the time of writing.