AI agents inside the logistics company

What they can read, what they can change, and who decides

IN BRIEF

01 Logistics and transport companies have put AI agents on the quote desk, the order desk and the customer chat. An American freight broker says more than 30 agents work across its network. An air cargo carrier enters emailed booking requests into its booking system by software and confirms them to the customer automatically.

02 The record is mixed. A Canadian tribunal held an airline to what its website chatbot told a passenger. A British parcel firm switched off the AI part of its chat after it swore at a customer. The suppliers are moving in different directions: one says “every exception routes to a human expert”, and another’s agents act “when the workflow and permissions allow”. None of the vendor pages we read commits to on-premises.

03 This paper is about the work around the shipment: the reading, checking and drafting done in customer service, bookings, shipping documents, customs, operations, the warehouse, the fleet, claims and finance. It sets out what an agent can read, how it reaches a logistics company’s systems, what it may change without a person, and what the rules already say about customers, workers and trade documents. It ends with seven questions to put to any supplier, and with a place to start.

04 The position throughout is simple. An agent prepares. A named person decides. Nothing the company is held to reaches a customer, a carrier or customs unseen. The agent runs on infrastructure the company controls.

IN THIS PAPER

01 Where logistics and transport companies are today 2
02 The work nobody has packaged 3
03 Three doors, one gate 4
04 What an agent may do 6
05 What the rules already ask 6
06 A worked example: one freight forwarder 8
07 Seven questions before an agent touches a shipment 9
08 Where to start 9

PART 01

Where logistics and transport companies are today

More than 30

AI agents one American freight broker says work across its network

32 seconds

for one of them to deliver a customer's price quote

About 90 seconds

for another to read an emailed tender and build the order

None

of the vendor pages we read commits to on-premises

Quotes and orders came first. C.H. Robinson says "more than 30 AI agents are now deployed at scale across its global network". One "delivers customer-specific price quotes in just 32 seconds". Another "Reads and interprets emailed tenders, including attachments, and builds orders in about 90 seconds" [1]. The page describes no review by a person.

Bookings are confirmed by software. Lufthansa Cargo uses "a software solution it developed internally to automatically enter booking requests received by email into the airline's booking system". The trade report adds: "Customers then receive a fully automated booking confirmation instantly" [2].

Customers meet agents too. Team Global Express in New Zealand has an agent that gives the delivery status "without human intervention", and "escalates the interaction to a human or raises a case" when a question is too hard [3].

Two warnings came from the customer desk. In January 2024 a customer told the British parcel firm DPD's chatbot to disregard its rules. It swore, and wrote that "DPD is the worst delivery firm in the world". DPD said: "An error occurred after a system update yesterday", and "The AI element was immediately disabled and is currently being updated" [4]. In February 2024 a tribunal in British Columbia held Air Canada to what its website chatbot had told a passenger about bereavement fares [5].

The suppliers disagree on how far an agent acts. Flexport's own page says an assistant can book "against a rate your AI agent just pulled, with the price, routing, and cargo details validated first"; a trade report has the company saying "every exception routes to a human expert" [6]. Manhattan Associates says its agents can, "when the workflow and permissions allow, execute the action across connected Manhattan Active solutions", with guardrails that set "which workflows require approval" [7].

Where they run is rarely said. None of the vendor pages we read commits to on-premises. Manhattan calls its platform "cloud-native" [7]; the other pages say nothing about hosting. Silence proves nothing either way, so the buyer has to ask: where it runs, which tools it may call, as whom, with whose approval, and what record is kept.

What the published accounts leave out. None of the deployments we read describes a step where a named person approves each quote, booking or message before it goes out.

Both public failures we found were chat that answered a customer with nobody in between.

PART 02

The work nobody has packaged

Every

library template we opened sends as soon as the workflow decides

Neither

of the two we quote shows a step where a person approves before a message or a record goes out

We listed the jobs done around a shipment, from the booking desk to the claims desk, and looked for each in the template libraries of the agent and workflow platforms. The libraries cover document validation and tracking updates. They thin out wherever a named person signs something.

WHERE TEMPLATES EXIST	WHERE NONE WAS FOUND
Customs document validation	**A freight invoice audited against the agreed rate**
Bill of lading checks with an emailed reply	**A cargo claim checked against the terms of carriage**
Shipment validation and freight documents	**A tariff code proposed for the classification specialist to decide**
Tracking updates written to a spreadsheet	**A dangerous goods declaration checked for the specialist**
	A demurrage or detention charge set against the free time agreed
	A carrier's licences and insurance checked before it is used
	A driver hours record check for the transport manager
	An incident report prepared for the safety manager to submit

Two findings matter more than the list. First, every library template we opened sends as soon as the workflow decides. One customs template sorts each shipment into clear, hold or reject and sends the exporter a "Detailed validation report with fix instructions". One bill of lading template drafts a reply and "sends it back to the original sender via Gmail" [8].

Neither shows a step where a person approves before a message or a record goes out [9].

Second, the templates we opened are built from hosted services: a hosted model, a hosted mailbox, a hosted chat or ticket service. That settles where customer and shipment data go before anyone has asked.

The gaps sit where the reading is slow and the decision already belongs to a named person. That makes them the safer place to begin.

PART 03

Three doors, one gate

An agent is only as useful as what it can reach. In a logistics company that means three kinds of thing.

Documents.

Operating procedures, rate cards, customer agreements, customs guidance, carrier terms, the claims procedure. These are indexed once as knowledge sources, with each reader's permissions kept, so an agent answers with the document it relied on and says when the documents are silent.

Systems of record.

Shipments, bookings, tracking events, orders, vehicles, receipts. Most are reached through an interface the company already runs or a carrier publishes. The company gives the platform the description of that interface, chooses which operations become tools, and decides which of them need approval.

Operations data for analysis.

On-time performance, transit times, stock counts, claims and costs, held in the data warehouse or a reporting database, and read only. The systems that control vehicles, cranes and sorters are not one of the doors.

All three pass one gate: every tool call is checked against the company's policy, which can allow it, record it, hold it for a person, or block it.

Where the company's interface checks the caller, the agent acts as the person using it and cannot claim another.

SIX WAYS INTO A LOGISTICS COMPANY'S SYSTEMS

	ROUTE	WHAT IT REACHES	WHAT TO KNOW
01	**A file the user uploads**	A bill of lading, a commercial invoice, a packing list, a customer's claim	Nothing is connected. The safest start
02	**A knowledge source**	Procedures, rate cards, agreements, customs guidance, carrier terms	Permissions are kept per reader
03	**An imported description of an interface**	Shipments, bookings, tracking events, orders, vehicles	You choose the operations. Changes wait for approval
04	**A reporting database**	Service performance, stock counts, claims, costs	Read only
05	**A server from the tool catalogue, run in your cluster**	Databases, web search, document conversion	It runs inside; check what each tool does
06	**Public sources**	Port notices, weather warnings, published schedules	Reads only, from the publisher

PART 03 · CONTINUED

59
interface descriptions taken from publishers and standards groups; the importer refused none

1,196
operations the importer found in them

608
of those operations read; 588 are sent as changes

199
of the 421 operations in one fleet telematics description change something

What is published. We took 59 interface descriptions from publishers and standards groups, counting each interface once: parcel shipping, fleet telematics, tracking, and the standards for ocean shipping, air cargo and supply chain events. The platform's importer refused none and found 1,196 operations [9].

What that exercise taught us. The open logistics interfaces are built to do things, not only to read. By method, 608 of the 1,196 operations read and 588 are sent as changes. One fleet telematics description alone carries 421 operations, and 199 of them change something. The ocean shipping standard's 31 files hold 116 operations, and 67 change something; in its electronic bill of lading interface it is 6 of 8.

What is not published. Transport management, warehouse, forwarding and customs systems publish no open description. Ocean carrier portals and two large parcel carriers keep theirs behind a sign-in. Where nothing is published, the company supplies its own description, or the agent reads from the data warehouse.

Vehicles and equipment. The safe design keeps the agent on the office side. It reads telematics and equipment data from a copy, and sends nothing to a vehicle, a crane or a sorter.

So choose the operations at import, start with the ones that read, and add nothing that books, issues, files or pays until the approval step has been seen working.

PART 04

What an agent may do

One rule runs through every agent in this paper: it prepares, and a named person decides.

01	**It reads** what the person using it could read, and no more.
02	**It drafts** the quote, the customs entry data, the discrepancy report, the claim decision note, with each statement tied to its source.
03	**It lists** what is missing, what does not match, what falls outside the procedure.
04	**It stops** before anything that changes a record or reaches a customer, a carrier, customs or a colleague. A tool that changes something waits for approval.
05	**It decides nothing about a person.** It does not allocate work to a driver, a courier or an operative, does not score them, and does not name anyone as the cause of an incident.

Four lines are drawn tighter than the rest.

Customers and what the company is held to.

An agent may draft the answer to “where is my shipment”, a delay notice or a quote, and show how each figure was reached. It tells a customer nothing binding unseen. A person sends every quote, notice and reply, and a new delivery date comes from operations.

Payments and claims.

An agent may check a carrier’s invoice against the agreed rate, or a cargo claim against the terms of carriage, and draft the note. It pays no invoice and settles no claim. Accounts payable and the claims handler decide.

Customs and bookings.

An agent may prepare the data for a customs declaration, propose candidate tariff codes with the reasons for and against each, and list what a booking request is missing. It files no declaration, confirms no booking and releases no cargo. The customs broker files; the booking desk confirms.

Drivers and staff.

An agent may check driving and rest records against the rules and list each possible breach with the record behind it, or draft a training note from a procedure. It allocates no work, scores no driver and assesses no one. The transport manager reviews each case.

PART 05

What the rules already ask

This part needs a lawyer’s read before it is relied on. It reports what the texts say; it is not advice.

What a company is held to

What the agent says, the company has said. In Moffatt v. Air Canada, a website chatbot told a passenger he could claim a bereavement fare after travelling; the airline’s policy did not allow it. As a Canadian lawyer’s note reproduces the decision, the tribunal wrote: “Air Canada suggests the chatbot is a separate legal entity that is responsible for its own actions”, and answered: “It should be obvious to Air Canada that it is responsible for all the information on its website.” It found that “Air Canada did not take reasonable care to ensure its chatbot was accurate” [5]. A news report puts the damages at “just over $650” [5]. It is one tribunal’s decision in one province, but the point travels: a quote, a delivery date or a liability statement from an agent is the company’s own.

People must be told. The European Union’s AI Act asks that systems “intended to interact directly with natural persons” be built so that “the natural persons concerned are informed that they are interacting with an AI system”, unless that is obvious [10].

PART 05 · CONTINUED

Workers

Allocating work or scoring a worker is high-risk. The AI Act lists as high-risk AI systems used "to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships" [10]. An agent that lists possible breaches in driving records for a manager allocates and scores nothing. One that chose which driver gets which job, or ranked drivers, would be read against this text.

The dates have moved. Regulation (EU) 2026/1744 set the high-risk duties to apply from "2 December 2027 as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III" and from "2 August 2028" for those tied to Annex I [11]. Worker management sits in Annex III, so its date is 2 December 2027. A high-risk system must be built so that it "can be effectively overseen by natural persons during the period in which they are in use" [10].

Platform work has its own directive. Member States must bring the Platform Work Directive into their law "by 2 December 2026". It requires digital labour platforms "to inform persons performing platform work" of "the use of automated monitoring systems or automated decision-making systems", and to "ensure sufficient human resources for the effective oversight" of their decisions [12]. Whether a given courier or delivery business is such a platform is for counsel.

Decisions about a person stay with a person. Under the GDPR, a person "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her", with stated exceptions [13].

Trade documents and customs

Freight information is going electronic, through certified platforms. The EU's electronic freight transport information regulation says that "competent authorities shall accept regulatory information made available electronically" by operators. The Commission gives the date: from 9 July 2027, "Member State authorities must accept information shared electronically by operators via certified eFTI platforms" [14].

An electronic bill of lading can carry legal effect. In the United Kingdom, "An electronic trade document has the same effect as an equivalent paper trade document", where "a reliable system is used" to identify and protect it [15]. No agent in this paper issues or transfers one.

Customs stays with the broker. We did not read customs law for this paper. The market points one way: one supplier of forwarding software describes "purpose-built AI agents to research and classify commodities automatically" under the heading "Human expertise remains essential" [16]. Here the agent prepares the entry data and the customs broker files.

Security and data

MARKET	WHAT WE READ	WHAT IT ASKS
European Union	NIS2 Directive, Annex I	Lists air carriers, airport and port managing bodies, railway undertakings and freight water transport companies as sectors of high criticality; they must take "appropriate and proportionate technical, operational and organisational measures" for the security of their systems [17]
European Union	NIS2 Directive, Annex II	Lists "Postal service providers", "including providers of courier services", among other critical sectors [17]
European Union	eFTI Regulation, Article 4	Operators that share information electronically do so "on the basis of data processed on a certified eFTI platform" [14]
European Union	AI Act, Annex III point 2	High-risk where AI is a safety component in "road traffic"; an agent that drafts and checks documents is not one [10]

We did not open customs law in any market, the rules on drivers' hours, or the rules in the United States, the Gulf or India. A company there should ask its own counsel.

PART 05 · CONTINUED

What the rules have in common

01	**The company answers** for what its agent tells a customer.
02	**Customers are told** when they deal with AI.
03	**A person stays in charge** of anything that allocates work to a worker or judges one.
04	**Filings and trade documents are legal acts,** and an agent that reads and drafts sits outside them.

PART 06

A worked example: one freight forwarder

Take a made-up freight forwarder that moves ocean, air and road freight: about 1,200 people, 14 offices, some 90,000 shipments a year. Nothing here is a customer's story, and every figure is illustrative; it is section 4 put to work.

01

On the documentation desk, a clerk uploads a bill of lading, a commercial invoice and a packing list. The agent lists two differences: the gross weight, and a consignee name spelt two ways. The clerk corrects the documents and releases them.

02

On the booking desk, a request arrives for a shipment with dangerous goods. The agent lists a missing class and a missing dimension against the booking rules. The desk returns the request and confirms nothing until both are there.

03

On the customs desk, the agent prepares the entry data from the commercial documents and lists a missing country of origin on one line. The customs broker checks the entry and files it.

04

In operations, the agent lists 23 shipments whose events show a missed milestone, with the customer and the cause recorded. The operations controller decides what to do about each.

05

On the claims desk, a customer claims for damaged cargo. The agent sets the claim against the terms of carriage and the shipment record, and notes that it arrived after the time limit for notice. The claims handler decides.

06

In accounts payable, the agent checks a carrier's invoice against the agreed rate and finds a fuel surcharge charged at last quarter's rate. Accounts payable disputes the invoice.

Every one of these reads documents or records the company already has, changes no record by itself, sends nothing to a customer, a carrier or customs, and leaves a record of who asked and what was shown.

PART 07

Seven questions before an agent touches a shipment

01 **Where does it run?**
On our infrastructure, in our private cloud, or in the supplier's service? Where is the model? Can it run with no connection to the internet?

02 **What can it read?**
Does it act as the person using it, with their permissions, or as one all-seeing account?

03 **What can it change?**
Which tools change a shipment, a booking, a customs entry, an invoice or a claim, and does each wait for a person?

04 **Can it speak for us?**
Show us that no quote, confirmation or message reaches a customer, a carrier or customs before a person has read and sent it.

05 **Who decides?**
Show us the step where a named person approves, and what the agent does when nobody has.

06 **What is recorded?**
Who asked, which tool ran, what was decided, and for how long is that kept?

07 **Can we stop it?**
One agent, one tool, or all of them, at once, by us.

PART 08

Where to start

Pick work where reading is slow, the decision stays with a person, and no shipment waits on the agent.

Shipping document checks

The agent lists every difference between the bill of lading, the invoice and the packing list. The documentation clerk corrects them.

Freight invoice audit

The agent checks each carrier invoice against the agreed rate. Accounts payable approves or disputes it.

Questions on your own procedures

Warehouse operatives ask what the site's own procedures say and get the answer with the step cited. No operational system is touched, so it can run on the first day.

One lane, one site, invented data first. Then beside the manual process, measured against it.

About Katonic AI

Katonic AI builds the platform that organisations use to build, run and govern AI agents on their own infrastructure: in their own data centre, in a private or sovereign cloud, or with no connection to the internet at all. The platform is in production with governments, banks, telecom operators and utilities. Katonic is certified to ISO 27001.

KATONIC.AI/SOLUTIONS/LOGISTICS

SOURCES

Read on 22 November 2026. Figures are the publishers' own and were not audited by us.

01 C.H. Robinson newsroom, "C.H. Robinson Scales Fleet of AI Agents Past 30", 12 June 2025. chrobinson.com

02 Air Cargo Week, "Lufthansa Cargo uses AI to process booking requests faster", 28 May 2025. aircargoweek.com

03 Salesforce customer story on Team Global Express New Zealand (written by the supplier). salesforce.com

04 The Register, "DPD chatbot blasts courier company, swears, and dabbles in awful poetry", 23 January 2024. theregister.com

05 Moffatt v. Air Canada, 2024 BCCRT 149, as reproduced in Barry Sookman, "Moffatt v. Air Canada: A Misrepresentation by an AI Chatbot", 16 February 2024, barrysookman.com (a lawyer's note; the tribunal's page would not open); and Global News, "Air Canada must pay B.C. man hundreds for chatbot error", 15 February 2024.

06 Flexport, MCP server page, flexport.com; and FreightWaves, "Flexport launches MCP Server for AI agents to book freight", 29 September 2026. freightwaves.com

07 Manhattan Associates, "Why ActiveAgents Are the Right AI for Supply Chain Commerce". manh.com

08 n8n workflow templates 13691 (customs clearance documents) and 16049 (bills of lading). n8n.io

09 Template libraries of agent and workflow platforms, searched 22 November 2026; and 59 interface descriptions fetched from their publishers and standards groups the same day and run through the platform's importer (Katonic research).

10 Regulation (EU) 2024/1689 (AI Act), Annex III points 2 and 4(b); Article 14(1); Article 50(1).

11 Regulation (EU) 2026/1744, 8 July 2026, recital 40 and the amended Article 113.

12 Directive (EU) 2024/2831 (Platform Work Directive), Articles 9(1), 10(2) and 29(1).

13 Regulation (EU) 2016/679 (GDPR), Article 22(1).

14 Regulation (EU) 2020/1056 (electronic freight transport information), Articles 4(2) and 5(1); and European Commission, eFTI Regulation page. transport.ec.europa.eu

15 Electronic Trade Documents Act 2023 (United Kingdom), sections 2(2) and 3(2). legislation.gov.uk

16 WiseTech Global (CargoWise), "How AI is changing export compliance: Where automation adds real value", 15 May 2026. cargowise.com

17 Directive (EU) 2022/2555 (NIS2), Article 21(1), Annex I point 2 and Annex II point 1.