AI agents inside the sales team

Who sends, where the data about people came from, and what an agent may change

IN BRIEF

01 Sales is the department where an agent's output reaches someone who did not ask for it. A first email. A follow-up. It goes out in the company's name, and the raw material is data about people. That is why the questions to ask first are not about where an agent runs. They are who sends, where the data about people came from, and what the agent may change.

02 The public material answers those questions differently. One vendor documents both. One of its agents has a mode in which "The agent sends outreach emails to customers". Of another it says "Sellers can review and send the draft email." Public workflow templates send email and connection invitations with no approval step, to contacts a scraper collected. Two suppliers publish the opposite: "Nothing sends or dials unless you tell it to", and outputs "should be reviewed by authorized personnel before any action is taken". Few of the pages we opened say where the agent runs, or whether the person who receives the email is told.

03 The record explains why the questions matter. France's privacy regulator fined a contact-data firm 240,000 euros for collecting contact details that users of a professional social network had chosen to restrict. The United States regulator's guide to the email law says it "makes no exception for business-to-business email". A tribunal in Canada held an airline to what the chatbot on its website told a passenger.

04 This paper is about the sales team's own work, from account research and first emails to quotes, the deal desk, the forecast and renewals. It sets out what an agent can read, how it reaches sales systems, what it may do without a person, and what the rules already say. It ends with seven questions to put to any supplier, and with a place to start.

05 The position throughout is simple. An agent prepares. A named person decides and sends. No agent sends an email, a message or a connection request, places a call or books a meeting. None enrols anyone in a sequence, moves a deal stage, changes a forecast figure, sets a price or commits the company to a term. Research is about companies. No agent scores a salesperson or reads mood. The agent runs on infrastructure the company controls.

IN THIS PAPER

01 Where sales teams 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 7
06 A worked example: one industrial equipment maker's sales team 9
07 Seven questions before an agent writes to a customer 10
08 Where to start 10

PART 01

Where sales teams are today

€240,000

the fine France's privacy regulator imposed on a contact-data firm for collecting contact details that users of a professional social network had chosen to restrict

$53,088

for each email, as we read the United States regulator's guide to the email law, which "makes no exception for business-to-business email"

The suppliers have arrived, and many sell the outreach itself. Vendor pages describe agents that research accounts, write and send email, answer replies and book meetings.

They disagree on who sends.

- Microsoft's documentation for one sales agent, a preview feature, says: "The agent sends outreach emails to customers". If there is no reply, "the agent sends up to four follow-up emails over the next three weeks". Then: "If customers aren't interested, the agent automatically closes the records as lost." The agent can pass a record to a human seller when it decides one is needed [1]. We found no approval step on the page.
- The same vendor documents another agent in a research-only mode. It researches a lead, checks the fit and drafts a first email. "Sellers can review and send the draft email" [2].
- One published workflow template runs daily. It finds people who match a profile, has a model write a cold email, and "then sends it via Gmail" [3].
- A second template sends connection invitations on a professional social network, and then "sends the AI-personalized outreach email directly from Gmail" [3].
- A third template does the opposite. A model proposes a score and an owner for each lead. "You validate every recommendation before anything gets updated" [3].
- Regie.ai says of its emails and call scripts: "Nothing sends or dials unless you tell it to." Rox's page says its outputs "should be reviewed by authorized personnel before any action is taken" [4].

Where the data about people came from is rarely the headline. In the second template above, a step named "Lead Scraping" uses a scraper that "collects contact details, emails" and profile data from a contact database [3]. Microsoft's research-only mode is narrower: its page says the agent "does not pass any Personally Identifiable Information (PII)" to the search service [2].

Few pages say whether the recipient is told. Relevance AI's documentation for its sales development agent says "we launch it into approval mode and then into full autopilot mode after a couple of weeks". It asks: "Will prospects know that they are talking to an AI Agent?" Its answer: "it is unlikely that your prospects will realise that it is an AI Agent." If a prospect asks, the page advises against denying it [5]. On the other supplier pages we opened, we found no statement on the point.

Few pages say where the agent runs. DealHub's page says: "If you have hosting-region or data-residency requirements, raise them during evaluation." A trade report of October 2026 describes one supplier, ASPR AI, giving customers the option to run its "sales agents inside their own cloud and on a large language model approved by their security team" [6]. So where it runs is still a question to ask every supplier. It is not the question that tells the products apart.

A privacy regulator has fined a contact-data firm. On 5 December 2024 France's data protection authority, the CNIL, fined KASPR 240,000 euros. KASPR's extension gave its customers the contact details of people with profiles on a professional social network. The CNIL said it had "received many complaints from people who had been canvassed" by the firm's customers. Some of those people had limited who could see their details. Collecting them anyway, the CNIL found, "exceeded what could reasonably be expected from people who register on a professional social network" [7]. The firm was ordered to stop, and to delete what it had collected that way.

PART 01 · CONTINUED

The email law does not stop at consumers. The Federal Trade Commission's guide to the United States law on commercial email says: "The law makes no exception for business-to-business email" [8].

A tribunal has held a company to what its agent said. In Moffatt v. Air Canada, decided on 14 February 2024 by British Columbia's Civil Resolution Tribunal, the chatbot on an airline's website gave a passenger wrong information about a fare. The airline argued it could not be held liable for what its chatbot said. The tribunal called that "a remarkable submission". It found the airline "did not take reasonable care to ensure its chatbot was accurate" and ordered it to pay $812.02 [9]. That case was about a website. A sales email carries prices and claims in the company's name too, which is why a person reads each one first.

We found no named, dated, independently measured result for a sales agent, and this paper quotes none as proof.

PART 02

The work nobody has packaged

We listed the jobs a sales team does and looked for each among the templates and prebuilt agents we opened. They are thick around the first email and the follow-up. We did not find them where the work is checking a draft, a record or a file for a named person.

WHERE TEMPLATES OR PREBUILT AGENTS EXIST	WHERE WE FOUND NONE
A cold email written and sent to a contact a search returned	**A check of the company's own do-not-contact list before a draft is written**
A connection invitation sent on a professional social network	**The source of each fact about a named person, kept beside the draft**
Follow-up emails sent on a schedule, and the record closed as lost	**What a person is told when their details came from somewhere else**
A lead's score and owner proposed for a person to approve	**The deals with a missing field, a past close date or no next step, listed for the owner**
A first email drafted for the seller to review and send	**A partner's deal registration checked against the programme rules**

PART 02 · CONTINUED

Two findings matter more than the list. First, in the templates that send, the message reaches a stranger before anyone on the sales team has read it [3]. Whether a person reads it is a setting, and whoever chooses it has decided what the company will answer for.

Second, the careful products show the better pattern. A draft lands in front of the seller, and nothing goes until a person sends it [2][4].

The gaps sit where the reading and checking 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 sales team that means three kinds of thing.

Documents.

The price book, the discount policy, product documents, the answer library, playbooks, standard terms. These are indexed once as knowledge sources, with each reader's permissions kept, so an agent answers with the passage it relied on and says when the documents are silent.

Systems of record.

Accounts, contacts, deals, quotes, calendars. Most are reached through an interface the company already runs. The company gives the platform its description, chooses which operations become tools, and decides which need approval.

Public sources and figures.

Company registries, filings and a company's own website are reached through web search. Pipeline, commits and usage figures come from a reporting database that is read only.

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 salesperson using it, so a salesperson sees their own accounts and a manager sees their team's.

SIX WAYS INTO A SALES TEAM'S SYSTEMS

	ROUTE	WHAT IT REACHES	WHAT TO KNOW
01	**A file the user uploads**	A request for proposal, a customer's contract paper, a questionnaire, meeting notes	Nothing is connected. The safest start
02	**A knowledge source**	The price book, the discount policy, the answer library, playbooks, the do-not-contact list	Permissions are kept per reader
03	**An imported description of an interface**	Accounts, contacts, deals, quotes, calendars	You choose the operations. Changes wait for approval
04	**A reporting database**	Pipeline, commits, closed deals, usage	Read only
05	**A server from the tool catalogue, run in your cluster**	Databases, web search, document conversion	It runs inside. The search words go to the search provider
06	**A company registry**	Legal name, registered address, officers, filings	Public. Through web search or the registry's own interface

261

public interface descriptions read, from 16 publishers; all 261 import

2,748

of the 4,625 operations in the 261 are sent as changes

What is published. We read 261 public interface descriptions from 16 publishers and ran each through the platform's importer. All 261 import, and three more were left out before the run because their format would not import. The 261 carry 4,625 operations, of which 2,748 are sent as changes, and the method alone cannot tell which only read [10].

What that exercise taught us. In these files a change is often an email sent, a contact enrolled in a sequence, a deal stage moved or an envelope sent for signature.

What is not published. Two of the 16 publishers account for 220 of the 261 files. The largest sales systems publish none a file address reaches. For those, the description comes from the company's own system, or the agent reads from the reporting database.

Web search. The search tool runs on a server inside the company's cluster. The words of the search go to the search provider. One vendor's documentation says of its own research agent: "it's possible that the information in the query might move across regions" [2]. So an agent searches for a company, not a person, and puts nothing from a customer record into the search.

The do-not-contact list. The list is the company's own. The agent checks it and says what it found. It does not decide whether a person may be contacted.

So choose the operations at import, start with the ones that only read, and add nothing that reaches a customer or changes a deal until the approval step has been seen working.

PART 04

What an agent may do

Two rules run through every agent in this paper. It prepares, and a named person decides and sends. And research is about companies.

01	**It reads** what the salesperson using it could read, and no more.
02	**It drafts** the brief, the email, the answer, the proposal, the pack, with each statement tied to its source.
03	**It lists** what is missing, what is out of date, what does not fit the policy, and what falls due.
04	**It stops** before anything that changes a record or reaches a prospect or a customer. A tool that changes something waits for approval.
05	**It does one job.** An agent is given the tools for one duty. The agent that checks a quote holds no tool that issues one.
06	**It scores no salesperson and reads no mood.** It gives no score and no rank to a member of staff, and it infers no emotion from a call or a text, the buyer's or the salesperson's.
07	**Claims carry sources.** What an agent drafts about a product, a price or a competitor shows where it came from, and a person stands behind it.

That gives 35 agents in nine areas: account research; leads and outreach; meetings; pipeline and records; quotes and proposals; the deal desk; forecast and reporting; accounts and renewals; enablement, partners and competitors. The full list is a separate document. Four lines are drawn tighter than the rest.

Research and named people.

An agent reads public company sources: registries, filings, the company's own website and news. About a named person it uses three sources only: what the seller already holds, what a company registry publishes about a company's officers, and what the buyer's own website says. It takes nothing from social network profiles, and the company buys no contact lists for it.

Records, forecast and price.

An agent may list the deals with missing fields and propose the updates a meeting implies. It moves no stage. It may assemble the forecast pack and show where the committed figures and the pipeline disagree. It changes no figure. It may check a draft quote against the price book and the discount policy and name the approver for each line. It sets no price and no discount, issues no quote and agrees no term.

Outreach.

An agent may draft a first email from the account brief and the messaging guide. It checks the company's do-not-contact list and says what it found. It sends nothing and enrols no one in a sequence. The salesperson edits and sends every email. Whether a person may be emailed or called at all depends on the country, and that decision is the company's.

Salespeople.

Reports are about deals, accounts and segments, and never rank salespeople. Meeting notes come only from transcripts the company holds of meetings recorded with the participants' knowledge.

PART 05

What the rules already ask

This part needs a commercial lawyer's read, and a privacy officer's, before it is relied on. It reports what the texts say; it is not advice. It does not say how any agent would be classified under any law. That is for counsel, system by system. Nothing in it says that a platform, or an agent, makes a company's outreach lawful.

Data about people

A person whose details came from somewhere else is told. Article 14 of the GDPR covers the case where "personal data have not been obtained from the data subject". The company gives that person its identity, its purposes, and "from which source the personal data originate, and if applicable, whether it came from publicly accessible sources". It does so "within a reasonable period after obtaining the personal data, but at the latest within one month". Where the data are used to write to the person, it does so "at the latest at the time of the first communication to that data subject". The article has stated exceptions [11].

A person can say stop. Article 21(2): "Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time". Article 21(3): after an objection, "the personal data shall no longer be processed for such purposes" [11]. This is why the agents here keep the source of each fact and check a do-not-contact list.

Email

In the European Union the starting point is consent, and business recipients are left to each country. Article 13(1) of the ePrivacy Directive says the use of "electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent". Article 13(5) applies the consent rule to "subscribers who are natural persons". For the rest, Member States ensure that "the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected" [12].

So the answer differs by country. In Germany, section 7 of the Act against Unfair Competition treats advertising by electronic mail without the addressee's prior express consent as an unreasonable nuisance in every case. A narrow exception covers a seller's existing customers [13]. We read the German text; the English here is ours. In the United Kingdom, regulation 22 of the Privacy and Electronic Communications Regulations "applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers". For them, marketing email needs a recipient who "has previously notified the sender that he consents" [14]. Who counts as an individual subscriber is for counsel.

In the United States the email law covers business email too. As we read it, the regulator's guide puts the penalty at "up to $53,088" for each email. A company that hires another to handle its email "can't contract away" its responsibility [8]. We opened no state law.

Calls

The Federal Communications Commission ruled in February 2024 that the restrictions on calls using an "artificial or prerecorded voice" "encompass current AI technologies that generate human voices", so such calls need the called party's prior consent [15]. No agent in this paper places a call.

PART 05 · CONTINUED

Telling the recipient

A person is told they are dealing with an AI system. Article 50(1) of the AI Act: "Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system", unless that is obvious to a reasonably well-informed person in the circumstances [16].

That duty applies from 2 August 2026. That is the Act's general date of application [16]. It is not the date for high-risk systems. Regulation (EU) 2026/1744 moved only those: the high-risk duties "shall apply from: (i) 2 December 2027 as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III; and (ii) 2 August 2028 as regards AI systems classified as high-risk pursuant to Article 6(1) and Annex I" [17].

Whether it reaches an email a person reads and sends is for counsel. In this paper a salesperson reads, edits and sends every message. We found no authority's view on that case, and this paper gives none.

Salespeople

Evaluating workers is on the high-risk list. Annex III of the AI Act lists, under employment, "AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, 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" [16]. Its date is 2 December 2027 [17].

Reading emotion at work is prohibited. Article 5(1)(f) bans "the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions", except for medical or safety reasons [16]. By its words that article is about the workplace and education. This paper does not say it covers a customer's mood. The agents here read no mood on either side of a call, as a design choice.

MARKET	WHAT WE READ	WHAT IT ASKS
European Union	GDPR, Article 14	A person is told who holds their details and where they came from, within one month at the latest [11]
European Union	ePrivacy Directive, Article 13	Prior consent for marketing email to natural persons; other subscribers left to each country [12]
United Kingdom	Privacy and Electronic Communications Regulations, regulation 22	Consent for marketing email to "individual subscribers" [14]
European Union	AI Act, Article 50(1)	People are told when they interact directly with an AI system [16]

PART 05 · CONTINUED

What the rules have in common

01	**The company answers for what goes out in its name,** whoever or whatever wrote it.
02	**A person is told where their details came from,** and can say stop.
03	**Email and calling rules differ by country,** and consent is often the starting point.
04	**Salespeople are protected too.** Evaluating workers is a listed use, and reading their emotion is barred.

PART 06

A worked example: one industrial equipment maker's sales team

Take a made-up company: a maker of industrial pumps that sells in three countries, with a sales team of 40. Nothing here is a customer's story, and every figure is illustrative; it is section 4 put to work.

01

A salesperson asks for a brief on a water utility she has never sold to. The agent reads the company registry, two annual filings and the utility's own website. The brief gives the group structure, a planned plant upgrade and the officers the registry lists, each line with its source.

02

She asks for a first email to the head of procurement, whose name is on the utility's website. The agent drafts it from the brief and the messaging guide, and checks the do-not-contact list. It reports that he is not on the list, and that his name came from the utility's website. She rewrites the opening and sends it herself.

03

A request for proposal arrives with 120 questions. The agent drafts answers from the answer library, cites the source of each, and marks 14 the library does not cover. The bid owner reviews every answer and submits the response.

04

A quote is drafted with an 18 per cent discount on one line. The agent checks it against the price book and the discount policy and reports that the line is above the 15 per cent a regional manager may approve. The sales director decides.

05

Before the forecast call, the agent assembles the pack: what each salesperson committed, the pipeline behind it, and four deals where the two disagree. The sales manager sets the forecast.

Every one of these reads sources the company already has or that a company has published, changes no record by itself, sends nothing, and leaves a record of who asked and what was shown.

PART 07

Seven questions before an agent writes to a customer

01 **Who sends?**
Which emails, messages, invitations or calls go out without a person reading them first? Is that a setting, and who holds it?

02 **Where did the data about people come from?**
Our own records, a registry, the buyer's website, a scraper or a bought list? Is the source kept with each contact?

03 **What may it change?**
Can it move a deal stage, close a record, change a forecast figure, set a price or a discount, or issue a quote? Does each of those wait for a named person?

04 **Is the recipient told, and can they say stop?**
If the agent writes to people itself, does it say it is AI? Is our do-not-contact list checked before every draft?

05 **Where does it run?**
On our infrastructure, in our private cloud, or in the supplier's service? Where is the model? Where do the words of a web search go?

06 **What is scored and recorded?**
Does anything score or rank a salesperson, or read mood from a call? What does the record hold, and for how long?

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 nothing reaches a customer on the agent's word.

Product and Policy Q&A
Salespeople ask what the documents and the price book say and get the answer with the source. No record is touched.

RFP Response
The agent drafts from the answer library and marks the gaps. The bid owner reviews every answer.

Record Check
The agent lists what is missing or out of date. The deal owner corrects each record.

One team, one process, 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/SALES

SOURCES

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

01 Microsoft Learn, "How the Sales Close Agent works" (Dynamics 365 Sales documentation; the page calls the feature a "production-ready preview"), page metadata dated 29 June 2026, updated 11 September 2026. https://learn.microsoft.com/en-us/dynamics365/sales/how-sales-close-agent-engage-mode-works

02 Microsoft Learn, "Responsible AI FAQ about the Research-only mode of Sales Qualification Agent" (Dynamics 365 Sales documentation), page metadata dated 3 April 2026, updated 30 April 2026. https://learn.microsoft.com/en-us/dynamics365/sales/faqs-sales-qualification-agent

03 n8n workflow template 19792, "Run autonomous SDR outreach with Apollo, OpenAI, Gmail, and Google Sheets" ("Last update 2 months ago" on the page; no publication date). https://n8n.io/workflows/19792 ; n8n workflow template 8449, "Automate cold outreach with Apollo, LinkedIn & Gmail using GPT-4" ("Last update 9 months ago" on the page). https://n8n.io/workflows/8449 ; Zapier template "Score and route inbound leads with AI", undated on the page (its question-and-answer data carries 23 February 2026), read 22 November 2026. https://zapier.com/templates/details/lead-scoring-review

04 Regie.ai, home page (questions and answers on RegieGO), undated, read 22 November 2026. https://www.regie.ai/ ; Rox, home page (legal notice in the footer), undated, read 22 November 2026. https://www.rox.com/

05 Relevance AI documentation, "Bosh the BDR agent", undated, read 22 November 2026. https://relevanceai.com/docs/agent/agent-examples/bosh-bdr-agent

06 DealHub, home page (frequently asked questions), page metadata published 15 October 2026, modified 10 November 2026. https://www.dealhub.io/ ; RuntimeWire, "ASPR AI puts its sales agents inside customer clouds to clear enterprise security reviews", 23 October 2026. https://runtimewire.com/article/aspr-ai-private-sales-agent-studio-ganesh-iyer

07 CNIL (Commission nationale de l'informatique et des libertés), "Data scraping: KASPR fined €240,000", 19 December 2024, on the decision of 5 December 2024. https://www.cnil.fr/en/data-scraping-kaspr-fined-eu240000

08 United States, Federal Trade Commission, "CAN-SPAM Act: A Compliance Guide for Business", dated August 2023 on the page, with the note "Edited January 2024 to reflect Inflation-Adjusted Civil Penalty Maximums"; the penalty figure is the one shown on the page on 22 November 2026. https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business

SOURCES continued

09 Moffatt v. Air Canada, 2024 BCCRT 149, Civil Resolution Tribunal of British Columbia, file SC-2023-005609, date issued 14 February 2024, paragraphs 2, 27, 28 and 44. The tribunal's own PDF: https://decisions.civilresolutionbc.ca/crt/crtd/en/525448/1/document.do

10 Templates and prebuilt agents of agent and workflow platforms, as opened for sources 1 to 5; and 261 interface descriptions from 16 publishers fetched 22 November 2026 and run through the platform's importer (Katonic research).

11 Regulation (EU) 2016/679 (GDPR) of 27 April 2016, Article 14(1), (2)(f), (3) and (5), Article 21(2) and (3). http://publications.europa.eu/resource/celex/32016R0679

12 Directive 2002/58/EC of 12 July 2002 (ePrivacy Directive), Article 13(1) and (5), consolidated version of 19 December 2009. http://publications.europa.eu/resource/celex/02002L0058-20091219

13 Germany, Gesetz gegen den unlauteren Wettbewerb (UWG), section 7(2) no. 2 and section 7(3), current text as shown on 22 November 2026. https://www.gesetze-im-internet.de/uwg_2004/__7.html

14 United Kingdom, Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426), regulation 22(1) and (2), text as shown on 22 November 2026. https://www.legislation.gov.uk/uksi/2003/2426/regulation/22

15 United States, Federal Communications Commission, Declaratory Ruling FCC 24-17, CG Docket No. 23-362, adopted 2 February 2024, released 8 February 2024, paragraph 2. https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf

16 Regulation (EU) 2024/1689 (AI Act) of 13 June 2024, Article 5(1)(f), Article 50(1), Article 113, Annex III point 4(b). http://publications.europa.eu/resource/celex/32024R1689

17 Regulation (EU) 2026/1744 of 8 July 2026 (Official Journal 24 July 2026), the replaced Article 113 point (c). http://publications.europa.eu/resource/celex/32026R1744