AI agents inside the developer and the contractor

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

IN BRIEF

01 Contractors, landlords and property managers have put AI assistants to work. One large contractor built its own on “our private Microsoft Azure environment”. Another is trialling agents that review inspection and test plans. One property firm says “More than 47,000” of its professionals have used its assistant.

02 The record is mixed. A firm that scored rental applicants agreed to pay “over $2.2 million” to settle a discrimination case. The suppliers are moving in different directions: one says its agents “never take action without sign-off”, and another describes agents that answer prospects and create work orders, with no approval step stated. None of the vendor pages we read states an on-premises or customer-cloud option.

03 This paper is about the company’s own work: the reading, checking and drafting done by staff in bids, commercial, design, site delivery, safety, handover, leasing, facilities and finance. It is not about anything that screens a tenant, sets a rent or directs a site worker. It sets out what an agent can read, how it reaches a project’s and a property’s systems, what it may change without a person, and what the rules already say about building records, tenants, contract notices and workers. 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 reaches a tenant, a buyer or a subcontractor unseen, and no agent issues a notice, certifies a payment or signs off an inspection. The agent runs on infrastructure the company controls.

IN THIS PAPER

01 Where builders, landlords and property managers are today 2
02 The work nobody has packaged 3
03 Three doors, one gate 4
04 What an agent may do 5
05 What the rules already ask 6
06 A worked example: one developer and contractor 8
07 Seven questions before an agent touches a project 9
08 Where to start 9

PART 01

Where builders, landlords and property managers are today

47,000
of one property firm's professionals, and more, have used its assistant

Three
warnings, all from rented housing in the United States

Two of four
supplier pages we read say a person reviews before anything goes out

None
of the vendor pages we read states an on-premises or customer-cloud option

Contractors began with their own staff. Skanska said of its internal assistant: "Built on our private Microsoft Azure environment, Skanska Sidekick harnesses the advanced language capabilities of the GPT-4 model" [1]. Balfour Beatty said its office assistant "will operate securely within Balfour Beatty's compliant and confidential IT environment". It is also trialling agents for "early-stage reviews of Inspection and Test Plans (ITPs)" [2].

Property firms began there too. JLL said of its own assistant: "More than 47,000 JLL professionals have already used the tool" [3]. The property products that followed go further: they talk to prospects and tenants.

Three warnings, all from rented housing in the United States. A tenant-scoring firm settled a class action, "agreeing to pay over $2.2 million and roll back certain parts" of its screening products, with no admission of fault [4]. A fair housing group sued a landlord and a software company, alleging that applicants on housing assistance "were systematically rejected through the use of preprogrammed conversational artificial intelligence (AI)" [5]. The Department of Justice filed a proposed settlement with RealPage over software that, as alleged, "relied on nonpublic, competitively sensitive information shared by landlords to set rental prices" [6]. No agent in this paper screens a tenant or sets a rent.

The suppliers disagree on how far an agent acts. Procore says its "agents never take action without sign-off" [7]. Document Crunch offers "Submittals, notices, and RFIs ready for review" [8]. AppFolio says one of its agents "self-sufficiently diagnoses and prioritizes resident maintenance requests" and creates work orders, and does not say whether a person approves first. Entrata's page offers to "Automate leasing, payments, and renewals" and is silent on approval [9].

Where they run is rarely said. None of the vendor pages we read states an on-premises or customer-cloud option. So the buyer has to ask: where it runs, which tools it may call, as whom, with whose approval, and what record is kept.

Two halves of one market. In construction, the published examples draft for a professional who signs. In rented housing, they talk to the public and act on the reply, and all three warnings come from there. A company that develops, builds and manages holds both halves, and needs one set of rules for both.

What the published accounts leave out. Two of the four supplier pages we read say a person reviews before anything goes out.

None describes who approves a change to a project record or a tenancy record.

PART 02

The work nobody has packaged

All three
property templates we opened send to tenants and vendors with no approval step described

Hosted
services are what all three are built from: form, model, mailbox, spreadsheet

We listed the jobs done around a project and a building and looked for each in the template libraries and prebuilt agents of the agent and workflow platforms. They cover tenant requests, leasing enquiries and routine site documents. They thin out wherever a named person certifies, accepts or signs.

WHERE TEMPLATES OR PREBUILT AGENTS EXIST	WHERE NONE WAS FOUND
A tenant's maintenance request classified and sent to a vendor	**A tender pack summarised for the bid manager**
Rent reminders and overdue notices sent to tenants	**A subcontractor's payment application checked before the surveyor certifies**
Replies to prospects, with showings booked	**A method statement or a permit to work checked against the site rules**
Work orders created from a resident's request	**A handover set checked against the contract's list**
Requests for information drafted for review	**A building's safety record checked against the list its duty holder must keep**
Submittals checked against the specification	**Planning conditions summarised with each trigger and date**
Daily logs built from site photos and messages	**A lease summarised with each date and its clause**
Contracts checked for risk, with notices drafted for review	**A disputed service charge checked against the lease**

Two findings matter more than the list. First, all three property templates we opened send to tenants and vendors with no approval step described. One "Sends acknowledgment to tenant and work order to vendor via Gmail", and is promoted as working "with zero manual follow-up". Another sends rent reminders and overdue notices to tenants. In the third a person appears only when no vendor matches: the workflow will "email the admin so a human can step in" [10].

Second, all three are built from hosted services: a hosted form, a hosted model, a hosted mailbox, a hosted spreadsheet. That settles where tenants' data goes before anyone has asked [11].

The gaps sit where the reading is slow and the decision already belongs to a named professional. 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. On a project or in a property portfolio that means three kinds of thing.

Documents.

Contracts, specifications, site rules, leases, operating and maintenance manuals. These are indexed once as knowledge sources, with each reader's permissions kept, so an agent answers with the clause it relied on and says when the documents are silent.

Systems of record.

Project documents and issues, the programme, cost records, tenancies, work orders, compliance records. Most are reached through an interface the company already runs. The company gives the platform the description of that interface, chooses which operations become tools, and decides which of them need approval.

Project and portfolio data for analysis.

Cost, progress, defects, lease dates and maintenance history, held in the data warehouse or a reporting database, and read only. Building controls and site plant 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 PROJECT'S AND A PROPERTY'S SYSTEMS

	ROUTE	WHAT IT REACHES	WHAT TO KNOW
01	**A file the user uploads**	A tender, a contract, a submittal, a permit to work, a lease	Nothing is connected. The safest start
02	**A knowledge source**	Contracts, specifications, site rules, leases, building manuals	Permissions are kept per reader
03	**An imported description of an interface**	Project documents and issues, the programme, cost records, tenancies, work orders	You choose the operations. Changes wait for approval
04	**A reporting database**	Cost, progress, defects, lease dates, maintenance history	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**	Planning data, building regulations, regulators' guidance	Reads only, from the publisher

PART 03 · CONTINUED

15
public interface descriptions read; the importer refused none

14
are within the import size limit

548
operations in those 14

227
of those operations are sent as changes

What is published. We read 15 public real estate and construction interface descriptions and the importer refused none. 14 are within the import size limit and carry 548 operations, of which 321 read and 227 are sent as changes. The fifteenth is one construction management platform's whole description: 3,391 operations in a single file about twelve times the import size limit, so a company imports the part it needs [11].

What that exercise taught us. The open interfaces are built to do things, not only to read. Two in every five operations in the 14 change something.

What is not published. The large property management, facilities management, scheduling and construction cost systems publish no open description. Where nothing is published, the company supplies its own description, or the agent reads from the data warehouse.

Site and plant. The safe design keeps the agent on the office side. It changes no setting on a building's plant, and it directs nobody on site.

So choose the operations at import, start with the ones that read, and add nothing that issues, certifies, approves 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 summary of a contract, the daily report, the reply to a tenant, the check of a payment application, with each statement tied to its source.
03	**It lists** what is missing, what does not match, what falls due and when.
04	**It stops** before anything that changes a record or reaches a tenant, a buyer, a subcontractor, a client or an authority. A tool that changes something waits for approval.
05	**It decides nothing about a person.** It does not screen or rank a tenant, does not score a worker, and does not infer anyone's emotions.

PART 04 · CONTINUED

Four lines are drawn tighter than the rest.

Contract notices and certificates.

An agent may list the notices a contract requires and the dates they fall due, and set a payment application against the subcontract and the measured work. It issues no notice and certifies no payment. The contract administrator issues every notice, the quantity surveyor certifies, and a missed date stays theirs.

Tenants and applicants.

An agent may draft the reply to a tenant's question from the lease, the building guide and the account. It screens, scores and ranks no one for a tenancy, and it sets no rent. It sends nothing to a tenant unseen: a property manager reads and sends every reply.

Design and inspection sign-off.

An agent may set a submittal against the specification and check a permit to work against the site's procedure. It approves no design, issues no permit and signs off no inspection, and it submits nothing to a planning or building authority. The designer, the permit authority and the inspector decide.

Site workers.

An agent may draft a toolbox talk from a procedure, or the daily report from the site diary. It allocates work to no one and scores no one. The site manager directs the work and signs the report.

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.

Building safety and records

A higher-risk building's information is a legal record. England's Building Safety Regulator says: "You must keep a digital record of information about a building" if you are a client, principal designer or principal contractor on a higher-risk building, or an accountable person for a high-rise residential one. This is the record often called the golden thread [12].

The record must be controlled. The same guidance says the information must be "secure from unauthorised access" and "a building's single source of truth". During design and construction: "Your system should have version control so users can see any changes" [12]. An agent that lists what the record lacks changes nothing in it.

Tenants and applicants

Housing is not on the European Union's high-risk list. Credit scoring is. The AI Act lists as high-risk "AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score" [13]. A tenant check that scored creditworthiness would be read against this text.

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 [14].

People must be told. The AI Act asks that people who deal directly with an AI system "are informed that they are interacting with an AI system", unless that is obvious [13].

The American cases ended in terms, not rulings. The scoring case and the chatbot case were settled [4][5]. The proposed judgment would require RealPage to "Cease having its software use competitors' nonpublic, competitively sensitive information to determine rental prices in runtime operation" [6]. We did not check whether the court has entered it.

PART 05 · CONTINUED

Contracts and professional duty

A notice missed can be a right lost. An article on the NEC contracts' own site sets out the time bar in clause 61.3 for notifying compensation events: eight weeks for a contractor, seven for a subcontractor. In its worked example the client enforces the time bar, and the contractor loses the right to compensation for that event [15]. An agent may list each notice and its date. It sends none.

The surveyor answers for the output. The Royal Institution of Chartered Surveyors' standard, in effect since 9 March 2026, says members and firms "must therefore apply their professional judgement to make a decision about the reliability of the output of any AI system used that will have a material impact on the delivery of surveying services". That decision is prepared by or under "an appropriately qualified and named surveyor who accepts responsibility for its use" [16].

Workers and data

Allocating work to a person, or scoring one, is high-risk. The AI Act lists 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" [13].

The dates have moved. Regulation (EU) 2026/1744 says the date of application of the high-risk duties "is set to 2 December 2027 for AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and to 2 August 2028 for AI systems classified as high-risk pursuant to Article 6(1) and Annex I" [17]. Employment and credit scoring sit in Annex III, so their date is 2 December 2027.

Inferring emotion at work is banned outright. The AI Act prohibits "the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions", with an exception for medical or safety reasons [13].

MARKET	WHAT WE READ	WHAT IT ASKS
European Union	AI Act, Article 26(7)	Before a high-risk system is used at work, "deployers who are employers shall inform workers' representatives and the affected workers" [13]
European Union	GDPR, Article 32(1)	Controllers and processors "shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" [14]
England	Building Safety Regulator guidance	Building information must be "secure from unauthorised access" [12]
Worldwide, for RICS members and firms	RICS standard, section 3.1	"RICS-regulated firms that use AI systems must safeguard any private and confidential data they hold" [16]

We did not open the housing law of the United States, the tenancy and site safety law of the United Kingdom, or the rules in the Gulf, India, Singapore or Australia. A company there should ask its own counsel.

PART 05 · CONTINUED

What the rules have in common

01	**A person decides** anything that judges a tenant, an applicant or a worker.
02	**A named professional signs** the notice, the certificate, the design and the record.
03	**People are told** when they deal with AI, and nobody infers how they feel.
04	**Building, tenant and worker records need protecting,** which is easier where the company controls the system.

PART 06

A worked example: one developer and contractor

Take a made-up company that develops, builds and manages: about 2,300 staff, 14 live projects and 60 buildings under management. Nothing here is a customer's story, and every figure is illustrative; it is section 4 put to work.

01

In the bid team, a bid manager uploads a tender pack of 1,400 pages. The agent summarises the scope and the key dates and lists five risks the documents place on the bidder, each with its clause. The bid manager decides whether to bid.

02

In the commercial team, the agent reads a newly signed contract and lists 38 obligations and nine notices with a time limit, each with its clause. The contract administrator checks the list and issues every notice herself.

03

For the quantity surveyor, the agent sets a subcontractor's payment application against the subcontract and the measured work and lists four differences. The surveyor values the work and certifies.

04

In the design team, the agent sets a cladding submittal against the specification and lists two departures. The designer comments and returns it.

05

At handover, the agent checks 620 documents against the contract's list and finds 23 missing. The project manager decides whether to accept.

06

In the property team, a tenant questions a service charge. The agent drafts a reply from the lease, the budget and the invoices. A property manager edits it and sends it.

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

PART 07

Seven questions before an agent touches a project

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 project document, a cost record, a tenancy, a work order or a payment, and does each wait for a person?

04 **Can it speak for us?**
Show us that no notice, reply or instruction reaches a tenant, a subcontractor or a client before a member of staff 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 site or tenant waits on the agent.

Contract obligations summary

The agent lists every obligation, notice period and date with its clause. The commercial manager checks it against the contract.

Submittal review

The agent lists where a submittal departs from the specification. The designer decides.

Lease summary

The agent sets out the term, the rent and the dates with their clauses. The property team checks it.

One project, one building, 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/REAL-ESTATE

SOURCES

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

01 Construction Briefing, "Why Skanska launched a new AI assistant and how it plans to keep data secure", 29 February 2024 (the words quoted are Skanska's). constructionbriefing.com

02 Balfour Beatty, "Balfour Beatty unveils £7.2 million AI investment: transforming how Britain builds", 31 July 2025. balfourbeatty.com

03 JLL, "JLL Falcon kicks off new era of AI-powered CRE innovation", 29 October 2024. ir.jll.com

04 Associated Press, "Renter scoring firm agrees to pay $2.2 million to settle case", in Fortune, 21 November 2024. fortune.com

05 Open Communities, "Open Communities Reaches Resolution in Case Alleging AI Discrimination", press release, 31 January 2024. open-communities.org

06 United States Department of Justice, press release 25-1111 on the proposed RealPage settlement, 24 November 2025. justice.gov

07 Procore, AI page. procore.com

08 Document Crunch, home page. documentcrunch.com

09 AppFolio, Realm-X Performers announcement, appfolio.com; and Entrata, ELI+ page, entrata.com

10 n8n workflow templates 9649, 17971 and 15780 (property maintenance and rent). n8n.io

11 Template libraries and prebuilt agents of agent and workflow platforms, searched 22 November 2026; and 15 interface descriptions fetched from their publishers and standards groups the same day and run through the platform's importer (Katonic research).

12 Building Safety Regulator (England), "Keeping information about a higher-risk building: the golden thread", updated 18 September 2024. gov.uk

13 Regulation (EU) 2024/1689 (AI Act), Annex III points 4(b) and 5(b); Articles 5(1)(f), 26(7) and 50(1).

14 Regulation (EU) 2016/679 (GDPR), Articles 22(1) and 32(1).

15 Steve Goodwin, "Notifying compensation events and time bars: a fairer approach needed", NEC Contracts news, 18 October 2022. neccontract.com

16 Royal Institution of Chartered Surveyors, "Responsible use of artificial intelligence in surveying practice", professional standard, 1st edition, September 2025, sections 3.1 and 4.2. rics.org

17 Regulation (EU) 2026/1744, 8 July 2026, the recital on the dates of application.