

Your Data and the New Tools

Where your information actually goes when your team uses the new tools, what the terms tend to say, and what to watch for before anyone pastes a customer list into a chat box.

Inside

1. The three questions to ask about any tool
2. What the common tools do with what you type
3. Five things to watch for
4. Three ways a system can be built
5. A checklist before you sign anything



The short version

Three questions, every tool.

You do not need to understand how any of this works to protect your organization. You need to ask three questions about any tool before it touches your information, and you need an answer to each one that is a fact rather than a feeling.

1. Where does it go?

Your computer, their servers, or somewhere in between. "The cloud" is not an answer. Whose cloud, and in what country, is.

2. Who can see it?

You, your team, the vendor's staff, the vendor's other customers, or a court that subpoenas the vendor. Each of those is a different tool.

3. What happens if we stop?

Can you take it with you, in a form you can use? Does the tool delete it, keep it, or keep it under terms that can change?

And one more, for your own team

Which tools are your people already using on their phones, on personal accounts, with company information? The honest answer is usually "some."

Why this matters more than it used to

For twenty years, the software your organization used mostly stayed put. Your accounting was in one place, your email in another, and the vendor's interest in your data ended at storing it. The new tools are different in one specific way: many of them learn from what they are given. That is what makes them useful. It is also why the question of what you give them, and under what terms, now belongs to whoever is accountable for the data, not to whoever set up the account.

The tool is not the risk. Not knowing where the information went is the risk.



The common tools, plainly

What happens to what you type.

These are general patterns, not legal descriptions of any one product. Terms change, sometimes with a few weeks' notice. The point is to know which kind of tool you are looking at, so you know which questions to ask.

The kind of tool	What tends to be true	Safe for
Free and personal chat tools The version someone signs up for with a personal email	Anything typed in may be kept, reviewed, and used to improve the product unless a setting is turned off, and it is usually on by default. It sits on the vendor's servers under consumer terms.	General questions. Nothing with a customer's name, a price, or an employee's details in it.
Paid business versions Team or enterprise plans, and the tools built on top of them	Usually a written promise not to train on your data, and better controls. It still sits on the vendor's servers, under terms the vendor can change, and it is still theirs to hand over if a court asks them.	Most day-to-day use, once someone has read the terms and set the settings.
Tools connected to your systems Anything that asks to link to your email, books, calendar or CRM	The permission screen is the contract. Many ask for far more access than the job needs. Read what it asks for before clicking Allow, and know how to revoke it.	The specific job it was connected for, with the narrowest access that gets it done.
A system built for you and hosted for you Custom work on a managed platform	Business-grade infrastructure with written terms. The builder sees only what is needed to support it. You should get a plain map of where every record lives.	Most multi-site and cloud-first operations. Ask for the map.
A system on hardware you control In your building, or a private cloud only you can reach	Nothing leaves. Nothing is shared. Nothing is subject to someone else's terms or someone else's lawsuit. Costs more up front, and needs someone responsible for the box.	Regulated work, public records, and anyone whose records cannot leave.

The one thing to do this week. Ask your team, without blame, which chat tools they use and what they have pasted into them. Then give them one that belongs to the company, with the right settings, so the customer list has a safe place to go.



Watch for

Five things that should stop the conversation.

1. The vendor cannot say where the data lives.

Not "it is secure." A place. If the person selling it does not know, nobody at the company you are about to trust with your records knows either.

2. The tool wants more access than the job needs.

A tool that drafts email replies does not need to delete email. A tool that reads invoices does not need to send money. Read the permission screen the way you would read a lease.

3. There is no way to get your information out.

Every real tool has an export. If yours does not, the information is not yours in any practical sense, whatever the terms say.

4. Your team is already on personal accounts.

This is the most common risk and the least discussed. The customer list has probably already been pasted somewhere. The fix is not a ban. Bans get ignored. The fix is a company account with proper terms, so there is a right place to put things.

5. The terms can change and you would not know.

Consumer terms shift with a few weeks' notice, and the notice goes to whoever signed up, which may be an employee who left. Business terms are more stable, and someone at your company should be the one who receives them.

If your work is regulated

Medical and dental offices, law firms, municipal departments and police, schools, and companies doing defense work each have rules about where records may sit and who may see them. Those rules follow the data, not the tool. A new tool does not get an exception because it is new. For many of these organizations the right answer is that nothing leaves hardware they control, and a good builder will bring that up before you do.



The three ways

How a system can be built, and what each means for your data.

When we build something for an organization, it lands in one of three places. Each is right for someone. The mistake is not knowing which one you are getting.

	Inside the systems you already run	In your own cloud tenant	On hardware you own
Where the data lives	Your existing systems. Nothing moves.	Your enterprise account, under your agreement.	Your building, or a private cloud only you can reach.
Who can see it	You, and anyone you already authorized.	You, and the builder only to support it.	Only you.
Internet required	Yes.	Yes.	Optional.
If you part ways	Nothing changes. It was always yours.	Your tenant. You revoke the builder's access.	It never left.
Usually right for	Automation inside an ERP or case system.	Multi-site reporting on cloud data.	Regulated data and public records.

Half the organizations who ask about the third option do not need it. A well-built system on the first or second is enough, and it should be said plainly when that is the case.

The line that matters

Whoever builds for you should be able to tell you, in plain language, where every record lives and who can see it. If they cannot answer that clearly, they have not built it right, whatever else it does.

Owning versus renting

Your organization's twenty years of jobs, records and correspondence can become a private model on hardware you control that never sends anything out. For some that is worth a great deal. For many it is more than they need today. Both are fine. The wrong answer is renting without knowing you are renting.

**Before you sign**

Ten questions for any tool or vendor.

Print it. Check what you can answer with a fact. Anything unchecked is a question for the vendor before money moves.

- ☐ We know where the data is stored: which company, which country, and whether it is on our hardware.
- ☐ We know who at the vendor can see it, and why.
- ☐ We have read whether the vendor uses what we type to improve their product, and turned that off if we can.
- ☐ We know what happens to our data if we cancel, and how we get it out.
- ☐ We know what the tool is allowed to do in our other systems, and how to revoke that.
- ☐ Someone at our company, not a former employee, receives the vendor's notices about changes to terms.
- ☐ Our team has a company account to use, so nobody needs a personal one for work.
- ☐ If our work is regulated, the vendor raised that before we did.
- ☐ We asked what the vendor would not recommend for us, and got a real answer.
- ☐ We have a plain map of where every record lives, in writing, before anything went live.

Ten checks is not the goal. Knowing which ones are unchecked is. A company that knows it is renting, and why, is in a fine position. A company that thinks it owns something it is renting is not.



Want the map for your organization?

Thirty minutes. Tell us which tools your team uses and what runs your operation. We will tell you where your information is actually sitting today, what is worth changing, and what is not. If everything is fine, we will say so.

**Schedule a meeting at rhodeislandintelligence.com/schedule
Or call or text 401-541-2747. You will get a person.**

Rhode Island Intelligence designs, builds and deploys private AI, process automation and robotics for manufacturers, municipalities, practices and firms with complex operations and information that cannot leave the building. Started by an operator who ran his own company for fifteen years. Cranston, Rhode Island.

Building for what's next.