

How Zapier keeps HR data safe

HR handles some of the most sensitive data in the company. If governance makes AI safe enough for HR, it makes AI safe enough for anyone. These are the three controls HR and IT teams ask about first.

1Enterprise

Action Restrictions

Control which operations each team can run inside an app. You approve the app, then decide what workflows and AI are allowed to do in it. Rules apply across Zaps, Agents, and MCP. IT chooses which apps are allowed at all.

2Enterprise Advanced

Workspaces

HR data stays in HR's space, not mixed with other departments. Each team gets its own workspace with its own permissions, apps, and connections, and IT keeps visibility across all of them.

3All plans

AI Guardrails

You choose to add it to any workflow (not as a company-wide setting). It checks text for 30+ types of personal data, like addresses, and returns a pass or fail. Checks for prompt injection, harmful language, and tone return a confidence score. You decide what happens next: stop the workflow, route it, or loop in a human.

Action Restrictions, for example:	
✓ Allowed	✗ Blocked
✓ Create candidate notes in your ATS	✗ Delete candidate records
✓ Read employee records in your HRIS	✗ Update employee records
✓ Draft emails to candidates	✗ Send emails without a person reviewing

On every Zapier plan

✓ SOC 2 Type II

✓ SOC 3

✓ GDPR

✓ UK GDPR

✓ CCPA

✓ Encrypted in transit and at rest

Zapier doesn't sell customer data. Enterprise customers are opted out of AI model training automatically.

Want to learn more?

Asset HistoryEnterprise

A record of every workflow run and the apps it touched, so you can answer "what did that touch?" in seconds. Admin actions are logged too.

Bring your own model (BYOM)Enterprise

Run Zapier Agents on AI models in your own cloud account, under your keys and agreements.

Managed App ConnectionsEnterprise

Company-owned HRIS and ATS connections keep workflows running when a recruiter leaves. Admins choose whether personal connections are allowed too.

Sign-in and accessEnterprise

SAML single sign-on, SCIM provisioning, role-based access, and domain restrictions that block personal accounts.

Next step: send this to your IT, security, or legal team. For a full review, ask your Zapier account team for the SOC 2 report, or see [Zapier Security and Compliance](#).