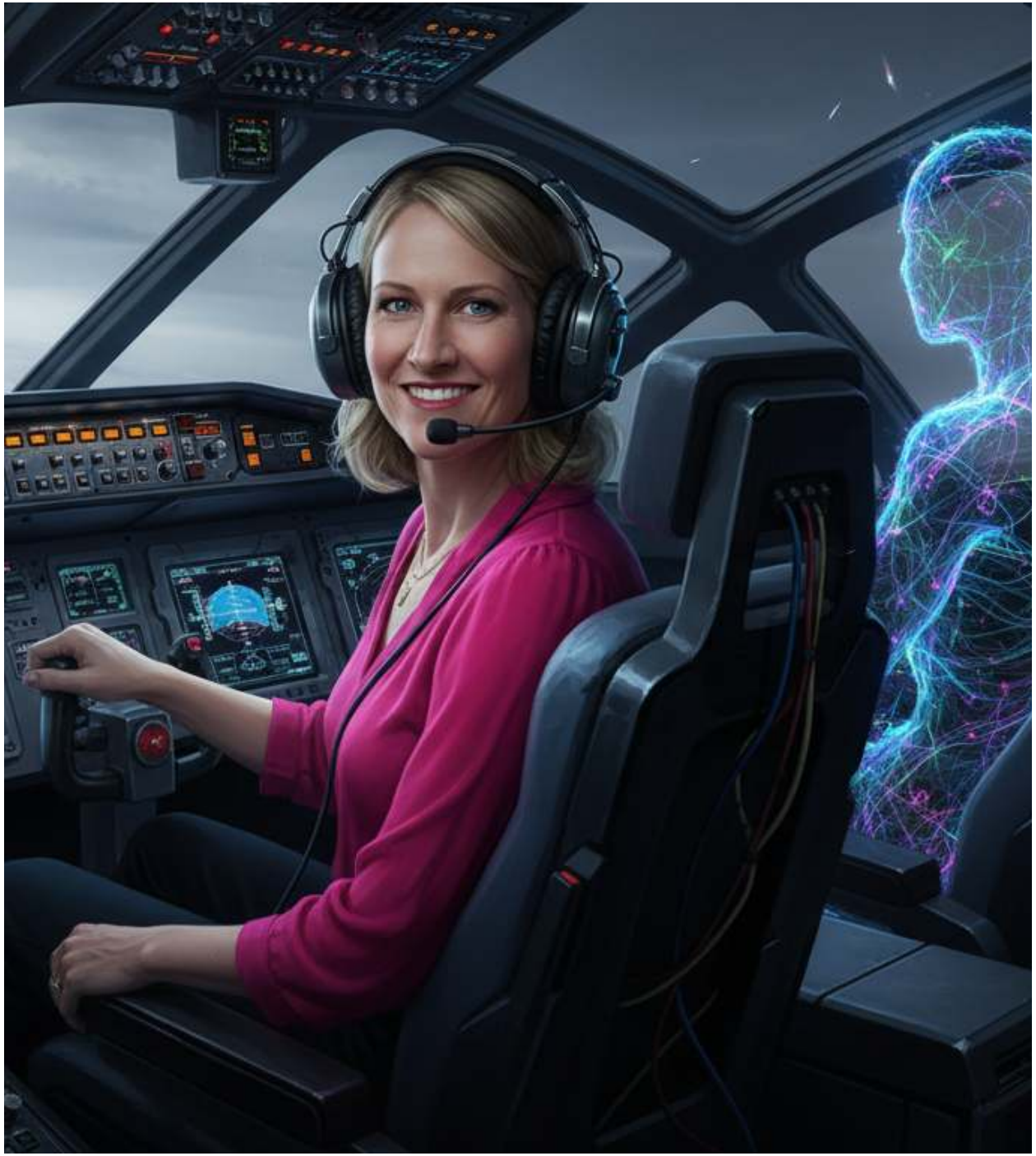
BRAND USA

BUILDING YOUR ORGANIZATION'S AI POLICY

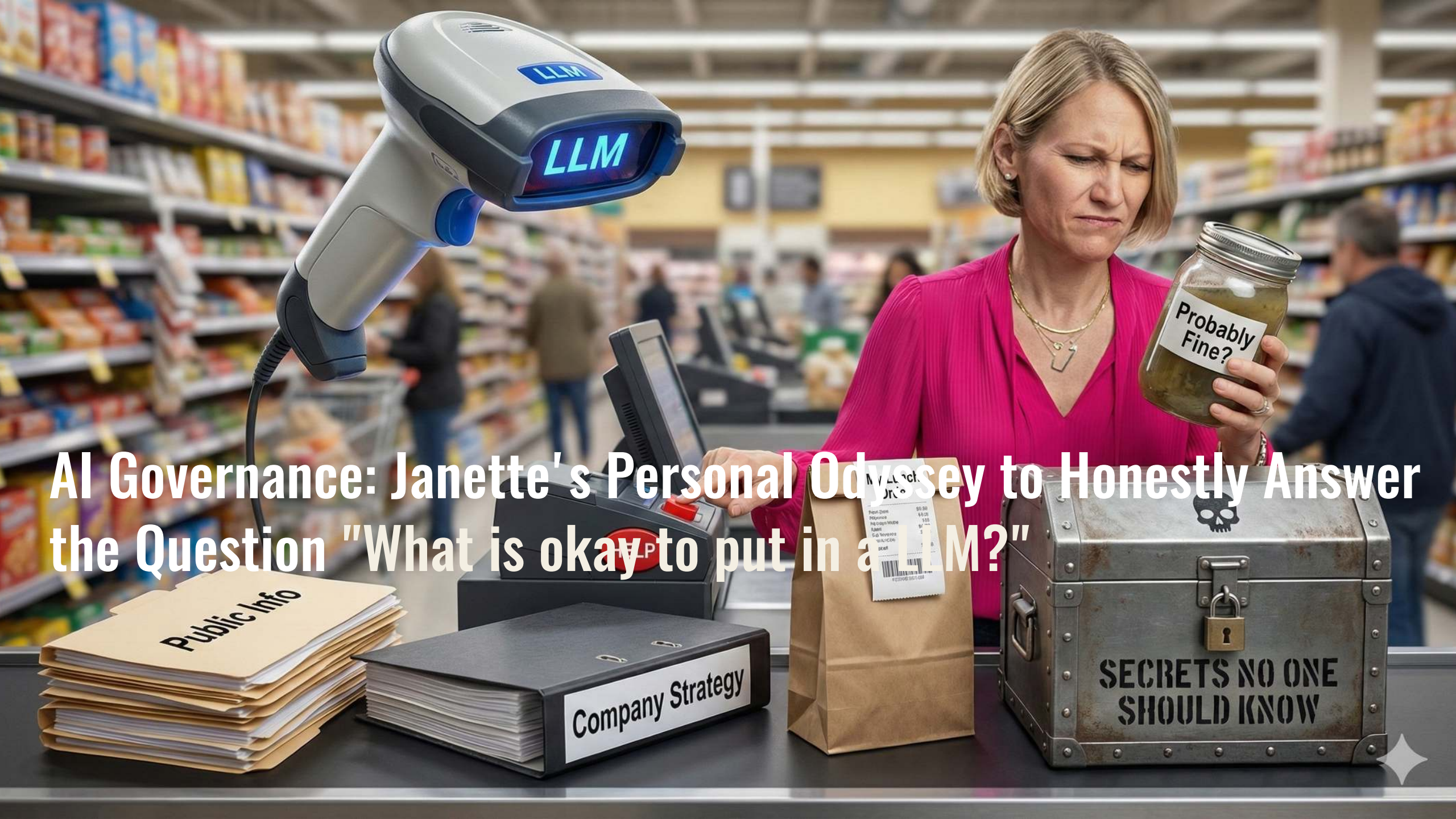
TRANSFORMING HOW THE WORLD DISCOVERS THE USA

December 2025



Brand USA will lead global destination marketing into the AI era by using intelligent systems to connect the world to the stories, people, and places of the United States—making discovery personal, inspiration effortless, and travel decisions frictionless.

- **EMPOWER OUR PEOPLE: Build AI fluency**
- **INSPIRE OUR INDUSTRY: Model responsible innovation**
- **REIMAGINE DISCOVERY: Make America discoverable and bookable**



AI Governance: Janette's Personal Odyssey to Honestly Answer the Question "What is okay to put in an LLM?"

Resources

- IAPP.org
- DrDavidPrivacy.com
- LuizasNewsletter.com
- OliverPatel.Substack.com
- White papers from Kara Franker & Roxanne Steinhoff

AI GOVERNANCE IS YOUR DMO'S PLAN FOR USING AI ETHICALLY, STRATEGICALLY, AND SAFELY.

Your staff wants to use AI ethically!

EY December 2023: AI Anxiety in Business Survey

Every AI policy answers three questions:

What are we PROTECTING?

People, partners, brand

What are we PROVIDING?

Secure tools, clear guidance, a person to ask

What are we EXPECTING?

Transparency, verification, human accountability


What are we PROTECTING?

What are we PROTECTING?

Data security

Protecting systems

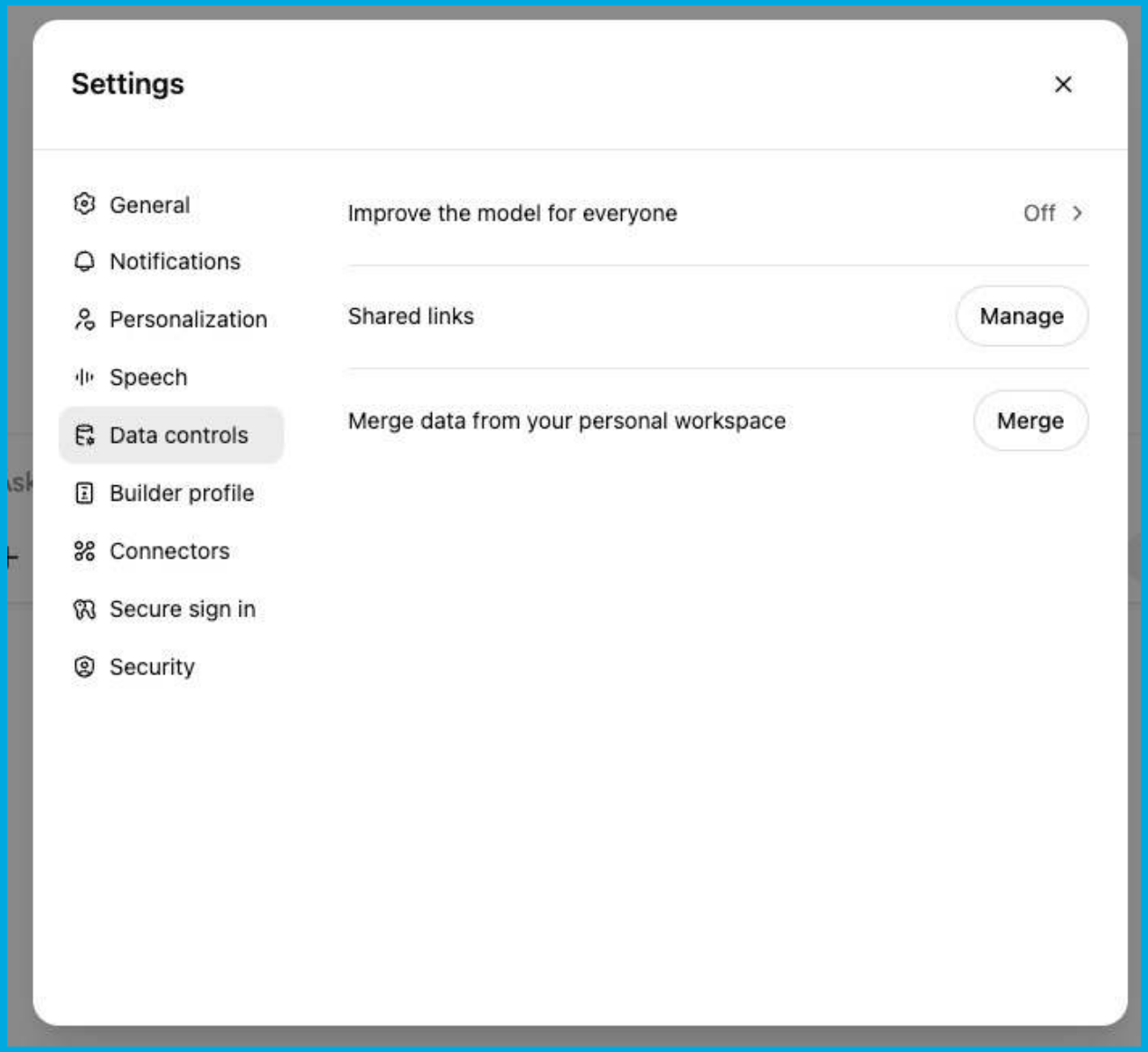
Data privacy

Protecting people

Content integrity

Protecting brand and community

- Ability to turn model training off
- Data encryption
- Data retention policies
- Admin controls
- Sub-processor transparency
- SOC 2 compliance



What are we PROTECTING?

Data security

Protecting systems

Data privacy

Protecting people

Content integrity

Protecting brand and community

Do not put PII into a LLM.

Do not put PII into a LLM.

You don't own someone's data - they own it (GDPR, CCPA).

People have the right to revoke your permission to use their data. But information that becomes part of the LLM's underlying training data can never be extracted. That is a violation of GDPR and CCPA.

Even with training data turned off, GDPR requires informed consent to be given for someone's PII to be entered into a LLM.

What are we PROTECTING?

Data security

Protecting systems

Data privacy

Protecting people

Content integrity

Protecting brand and community

The risks of putting external information (context) into an LLM

Permanence

Once inputs are in the training data, they can't be extracted

Applies to tools that train on your inputs

Regurgitation

The LLM could reproduce your content in someone else's response

Applies to tools that train on your inputs

Rights violation

You didn't have permission to share this data with a third party

Applies to licensed content, partner data, visitor PII

Do I have the right to share this information with a service provider?

Data type	Can I share with a service provider?
My own drafts, notes, ideas	✅ Yes
Public information	✅ Yes
Internal strategy docs	✅ Usually yes (check your org's cloud policy)
Licensed research reports	❌ Probably not without checking the license
Partner confidential materials	❌ Not without their permission
Visitor PII	❌ Not without consent (especially GDPR)
Employee HR data	❌ Almost never appropriate

The question is less "What is okay to put in a LLM?" and more "WHY are you doing it?" or "HOW are you using it?"

Lowering your risk of IP infringement (output)

Lower-Risk Use Cases

Internal strategic planning

Non-commercial educational purposes

Market and policy research

Internal governance and compliance work

Why These Carry Less Risk

They're non-public or non-commercial

They involve internal use, research or commentary

The AI output is not used to devalue the original IP

Does your use case qualify as "Fair Use" under US law? (input)

Purpose and character of use

- Non-commercial, educational, nonprofit purposes (such as internal strategy planning).
- Transformative uses (adding something new, insights, or repurposing for a distinctly different purpose).
- Internal use without distribution to the public.

Nature of the copyrighted work

- Factual or informational works (e.g., policy guidelines, governance documents, data).
- Works published or broadly disseminated publicly.

Amount and substantiality of use

- Using small portions or excerpts relative to the entire work.
- Avoiding the “heart” of the work (the central essence that makes the work valuable).

Effect on market or potential value

Little to no impact on the market value of the original content.

Internal use that doesn’t reduce demand or marketability of the original work.

Best practices to further reduce risk (output)

Explicit attribution

Transparency

What are we PROVIDING?

What are we PROVIDING?

Secure tools

Clear guidance

A person to ask

Provide secure (paid) tools for your staff.

ChatGPT Team

Claude Team

Gemini for Google Workspace

Microsoft Copilot

BYOAI risks

Security

- Data breaches with no centralized control to protect sensitive information
- Malware and phishing threats (through third-party AI browser plug-ins or fake AI apps)
- Privacy risks regarding GDPR and CCPA
- Employees retain company data after they separate from the company through their personal AI tool stack

Operational

- Fragmented tools
- Accuracy issues - hallucinations, uptime or usage limits, lack of guarantees of performance for free or personal tools
- Lack of oversight - no visibility into how decisions or content are being generated, no support from IT if the tool malfunctions or produces problematic results

Reputational

- Visitor trust - data breaches, offensive/incorrect responses to customers
- Legal fallout - Regulators could discover that employees were funneling client data into an unauthorized AI app. Lawyers in an IP dispute could discover that content that infringes on existing copyright was created in an unauthorized AI app.

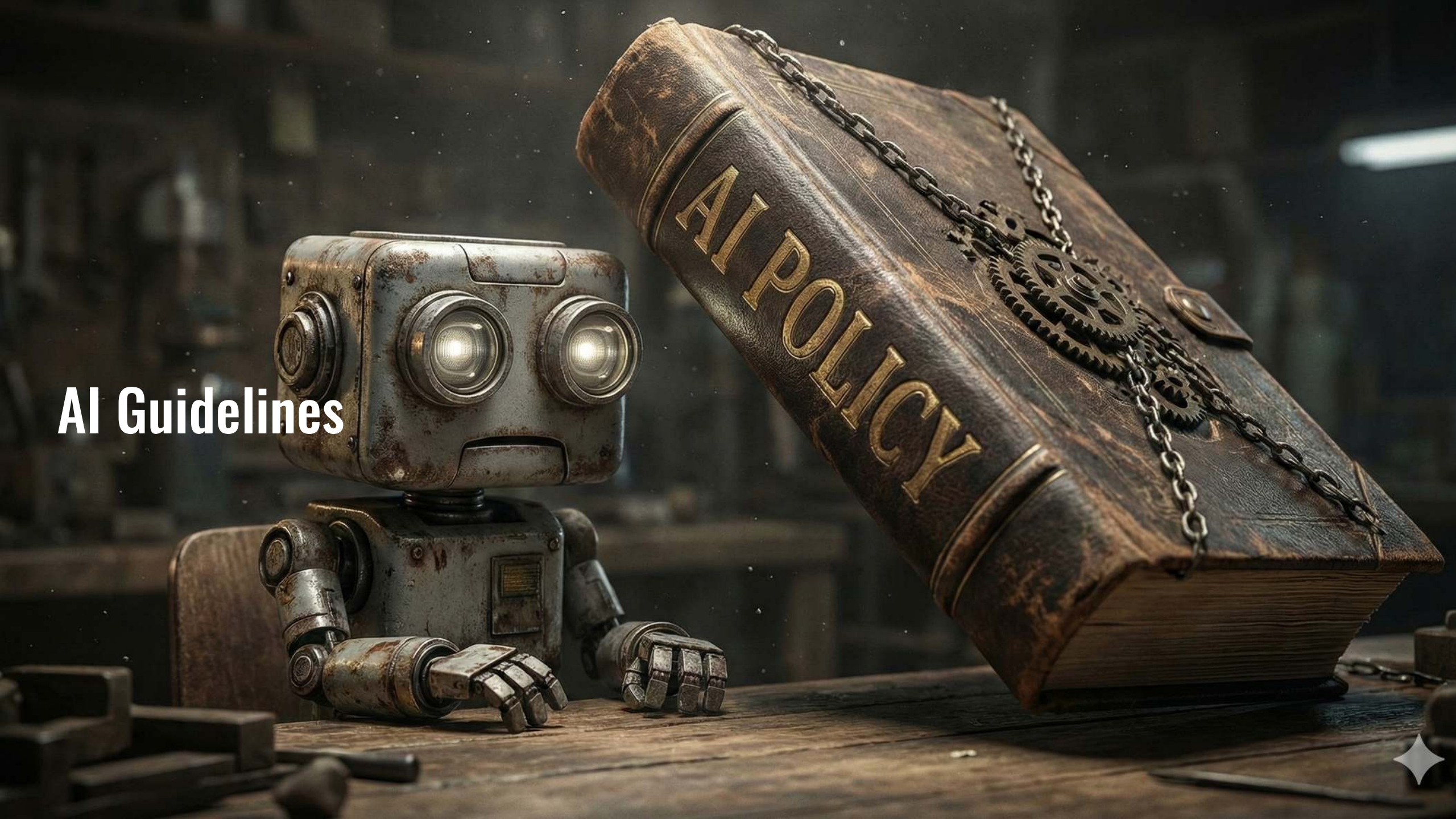
What are we PROVIDING?

- Secure tools
- Clear guidance
- A person to ask


What are we EXPECTING
DRAFT
NEEDS REVIEW
UNCERTAIN

What are we EXPECTING?

1. Transparency
2. Verification
3. Human accountability



AI Guidelines

Vision

What do you want AI to achieve for your organization?

Is your approach low-risk or high-risk?

Ethical Principles

How transparent will you be about AI use?

In what ways will your organization use AI?

Responsibility

How will you keep the human in the loop?

Confidentiality / Safety

How will your organization protect PII, confidential records and information you are licensing but do not own?

Governance / Accountability

How will your organization ensure compliance with your AI policy?

Who is the internal lead for AI oversight?

How will you train staff?

Practical Tips

What tools are allowed?

What are examples of permissible use cases?

Source: AI Opener for Destinations / Steinhoff Law / Miles Partnership / Group NAO

Brand USA AI Guidelines

Organizational AI Guidelines

Updated 12.9.24

Vision

Brand USA aims to set the global standard for responsible and innovative AI-powered tourism promotion. We are committed to leveraging artificial intelligence tools to advance our mission of driving international inbound tourism, fostering economic growth for communities and businesses, enriching travelers' experiences, and strengthening international diplomacy. Central to this vision is our dedication to education—empowering our staff and the broader tourism industry to embrace and effectively utilize AI tools for sustainable growth and shared success.

Transparency

Brand USA is transparent about our use of AI, sharing when AI has been used to substantially assist with a task or piece of content, and actively engaging stakeholders in conversation about our AI strategies and their impacts.

Internally, disclose when you have used AI to generate content to build trust and provide a teaching moment for colleagues. A sample credit line would be "These AI Guidelines were generated with support from ChatGPT-4o and edited by Janette Roush."

We embrace a culture of responsible experimentation, where we maintain control and understanding of the use of these tools while we develop new uses that drive efficiency, innovation or other outcomes in service of our mission.

Brand USA AI Guidelines

Responsibility

Keep the human in the loop. Generative AI is a tool, and we are responsible for the outcomes of our tools. For example, if autocorrect unintentionally changes a word, changing the meaning of something we wrote, we are still responsible for the text.

Fact check and review all content generated by AI, especially if it will be used in public communication, which could include social media, press releases, itineraries, presentations and external reports. Look for inaccurate information including links and references to events or facts, and for bias in the information presented. Remember that AI cannot “fact check” itself, and that it can inadvertently infringe copyright by producing text that closely resembles existing copyrighted material. It is a large language model, not a large knowledge model, and outside of the context you provide in a prompt it has no relationship to “truth.”

Brand USA is responsible for providing ongoing training in using AI tools for all staff, empowering them to use them confidently and safely.

Brand USA AI Guidelines

Confidentiality and safety

Do not enter personally identifiable information (PII) into a prompt; this includes names, phone numbers, email addresses and mailing addresses. The EU AI Act and pending state legislation requires an individual to explicitly consent to their information being entered into a prompt.

Do not put confidential or proprietary information into a prompt; this includes reports we receive through a license or subscription, trade secrets, confidential information shared with us by partners or other stakeholders, financial information about our operations and information about our employees. Please reach out to Jake Conte and Janette Roush if you have a question about a specific piece of information you would like to work with in a LLM; the third-party sharing agreements of these contracts could be amended to include these permissions.

We want to be careful with "BYOAI", or bringing your own AI tools to work. Some meeting notetaking tools, for example, ask for access to your calendar and email, and our technology team needs to vet the security of tools that are given access to Brand USA systems. Additionally, our legal team needs to review the terms and conditions of tools that are processing Brand USA content.

Company-provided accounts for ChatGPT Team and Claude Team protect our data with SOC 2 compliance (making our information more secure in the cloud where the language model processes your prompts) and by not training future language models on the data we input. While more secure than free versions of these accounts, the paid accounts do not override the specific considerations of GDPR or third-party sharing agreements for licensed reports.

Governance and accountability

Employees are encouraged to provide feedback or report concerns regarding AI use to ensure continuous improvement and compliance for our program. Please reach out to Janette, your manager or HR to discuss.

This policy will be reviewed annually or as needed, based on the evolution of AI technology and the regulatory landscape. Any changes to this policy will be communicated to all employees.

Custom GPT

AI Governance Coach for DMO Leaders

Working with vendors

Clearly define data ownership, access and privacy in partner agreements

Require partner to disclose their use of visitor data (including PII)

How are your vendors using AI? Are partners mentioning AI guidelines in contracts?

Sample AI Contract Checklist

This is not legal advice!

- **Transparency**
  Agency clearly identifies when AI-generated content is used
- **IP and Content Ownership**
  Contract explicitly states who owns AI-generated content
- **Third-Party IP Usage**
  Agency agrees to use only licensed, owned, or appropriately sourced IP
- **Incident Reporting**
  Agency agrees to promptly report any AI-related problems
- **Data Privacy and Security**
  Agency follows clear rules for handling sensitive data
- **Human Review**
  Agency commits to human oversight before publishing AI-created outputs

Procurement Checklist

"What to ask - and who to ask - when you buy risky tools from strangers!"

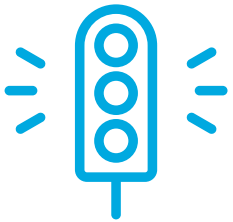
-Laura Haaber Ihle, AI ethicist

1. **Upload Terms of Use and Privacy Policy to ChatGPT**
2. **Prompt "What should concern my DMO regarding these Terms of Use / Privacy Policy?"**
3. **Security: Do they offer SSO? How is your data encrypted?**
4. **Privacy: Do they use your content to improve their service? Does your DMO own the outputs?**

What Leadership Must Do

Your To-Do List

Empower Staff, but Set Limits



Approve and Communicate Guidelines

Oversee Vendor and Tech Stack Risks

Set the Tone

BRAND USA

REGISTER FOR UPCOMING AGENTS OF CHANGE WEBINARS

The CRIT Framework: Advanced Prompting Techniques for Tourism Marketing

January 6th 1:00pm EST

THEBRANDUSA.COM/EVENTS/WEBINARS

BRAND USA

VIEW PAST WEBINARS

https://brand-usa-agents-of-change.vercel.app/

BRAND USA

THANK YOU

JROUSH@THEBRANDUSA.COM