EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

AI, Knowledge Ownership & Workplace Risk

WHOSE SKILLS ARE THESE ANYWAY?

AI, Knowledge Ownership, and the Emerging Workplace Risk

Maier Fenster
Patent Attorney
Head of Medical Device Dept.

Adv. Yehuda Neubauer
Head of Litigation

EHRLICH&FENSTER PATENT & TRADEMARK ATTORNEYS
EN&M EHRLICH, NEUBAUER & MELZER ATTORNEYS AT LAW
IPTRADE® AN EHRLICH INITIATIVE
iPatent®

Legal Disclaimer

- The purpose of this presentation is to communicate concepts. There is no guarantee that the information presented here is correct, complete or up-to-date.
- The information is not legal advice. Legal advice is when you apply law to facts in view of decisions.
- Go to a lawyer to get legal advice.
- Go to a patent attorney to get advice related to patents/Intellectual property.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

AI, SKILLS & AGENTS A FEW WORDS

AI and Skills are quietly converting tacit human knowledge into portable, documented, legally contested assets.

AI

Software systems that learn from data and generate outputs such as text, analysis, and recommendations that once required human expertise.

Key Risk

Third-party vendors (OpenAI, Anthropic, Microsoft, Google) process and often retain interaction data. Your confidential information may reside in infrastructure you do not control.

SKILLS

Accumulated know-how an employee encodes into prompts, workflows, fine-tuned models, and AI- assisted outputs, making tacit expertise explicit and portable.

Why It Matters

Built using employer data, systems, and time. Transforms what was in someone's head into a legible, exportable asset; often plain text files.

THE IMPLICATION

Together, AI systems and encoded Skills convert what was once informal, personal expertise into structured, documented, and legally contestable intellectual property.

Right Now

This is happening in most organizations today without ownership frameworks, without policy, and without employer awareness.

AI AGENTS

- Autonomous systems that act on instructions, execute tasks, draft documents, and interact with third parties with minimal human intervention.
- Operate on behalf of employees with limited oversight but full liability
- Each vendor has its own terms of service governing data use and retention
- Subcontractors, cloud providers, and freelancers may also be involved in the chain
- In this rapidly processing and changing field, there are also tools for managing groups of agents

In your organization today, employees are actively building personalized AI tools using employer data, employer systems, and employer time without a formal ownership framework in place!

The risks can be due to malicious acts, but most likely problems will be caused by honest or naive activities or simply confusion due to lack of framework

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

THE WORKER WHO LEAVES WITH MORE THAN A CARDBOARD BOX

When an employee walks out today, they may carry a fully documented, AI-encoded playbook of your most sensitive operational knowledge, and existing legal tools may not be adequate to stop it.

SOFTWARE COMPANY

Senior developer builds AI coding assistants trained on proprietary architecture, joins a competitor - personal AI tool goes with her.

SERVICE FIRM

Consultant encodes client relationship patterns, pricing logic, and proposal templates into AI workflows. The client list effectively travels inside the model.

MANUFACTURER

Process engineer uses AI to document production methods and supplier relationships (trade secrets) and exports the AI skill set on his last day.

R&D TEAM

Researcher's AI-assisted lab notebooks constitute a structured, legible record of years of proprietary research previously impossible to extract so completely.

The Core Problem

Know-how that was previously locked in someone's head is now legible, exportable, and reproducible AI has departed a potential trade-secret catastrophe for a single employee.

THE WORKER WHO ARRIVES WITH SOMEONE ELSE'S SECRETS

Every new hire is a potential conduit for a competitor's trade secrets, and your on boarding process is the last line of defense.

Hiring talent that brings AI-encoded know-how from a previous employer creates new legal and reputational exposure even when there was no malicious intent.

- Employees routinely import personal AI tools, custom prompts, and fine-tuned models built using prior employers' confidential data.
- A new hire's AI assistant may contain encoded trade secrets from a direct competitor —without either party realizing it.
- Onboarding procedures must now include AI hygiene as a standard step.

The Risks

Contamination	Teams inadvertently incorporate a competitor's secrets into your own work product.
Reverse Engineering	Structured AI outputs can reveal the underlying confidential data they were trained on.
Liability Risk	Receiving stolen trade secrets, even unknowingly, can constitute misappropriation under the DTSA.

Legal Context

The Defend Trade Secrets Act (DTSA)

Trade secret filings in U.S. courts have risen steadily since the passage of the DTSA in 2016, creating a growing body of precedent that now reaches AI-encoded know-how.

Filings have risen **steadily since 2016** and AI misappropriation cases are among the fastest-growing categories.

Liability can attach even when the receiving party had no intent to misappropriate.

AI Hygiene must be a standard onboarding checkpoint, not an afterthought.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

THE WORKER WHO NEGOTIATES OWNERSHIP

The talent market is shifting - **clarity on AI ownership is becoming a competitive differentiator**, not just a legal protection.

High-value employees are beginning to assert ownership over the AI tools they build and the most talented candidates will choose employers who offer clarity over those who don't.
Early disputes are emerging over who owns the custom prompt library, fine-tuned model, and AI-curated knowledge base.

No Policy = No Protection

Employers without a clear AI ownership position are vulnerable to ad hoc disputes at the worst possible time —employee exit.

Overreaching Backfires

Blanket claims to all AI outputs — including those built on general knowledge — are likely unenforceable and deter top candidates.

Leverage Asymmetry

The more indispensable the employee's AI skill set, the stronger their negotiating position — making clarity now far less costly than disputes later.

Disputes Are Already Emerging

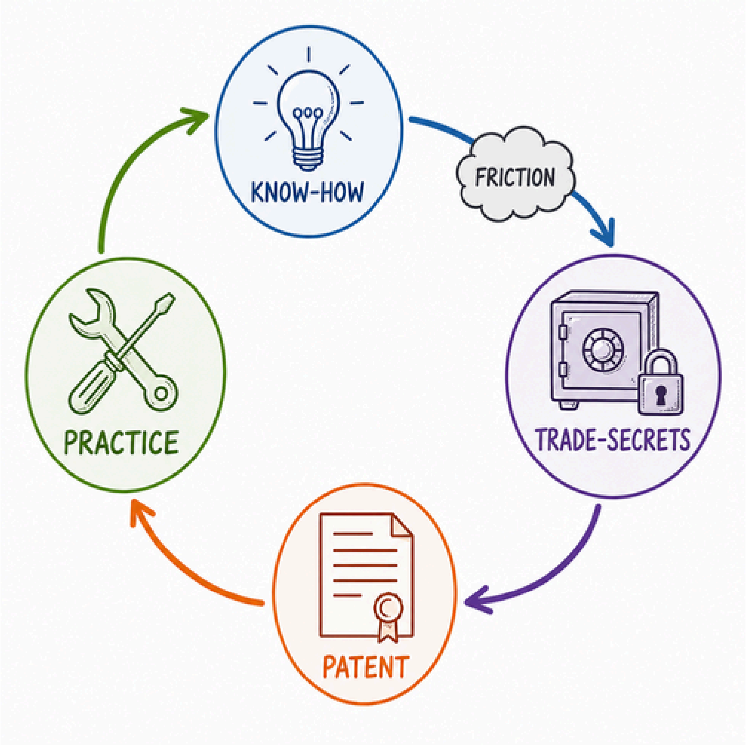
Early disputes are emerging on custom prompt libraries, fine-tuned models, and AI-curated knowledge bases — ownership frameworks are urgently needed.

Every day without a policy is a day of unresolved ownership, potential disputes are being created before employers act.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

THE KNOW-HOW CYCLE

- Traditionally, practicing an activity creates know-how which may be converted to various types of IP.
- This IP compounds in value over time; each cycle strengthens competitive position.
- No more: AI has made every stage faster, more legible,and more legally contested.
- The IP-power of know-how relied on friction - the difficulty of transferring it.
  AI demolishes this power by reducing friction.
- Employers accelerate this by requiring workers to use AI, hoping to replace workers with AI tools they helped build.



AI doesn't just accelerate the know-how cycle it eliminates the friction that once protected employers from knowledge leakage.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

OLD WAY VS. NEW WAY: THE EMPLOYEE WITH KNOW-HOW

The nature of employee know-how has shifted from something diffuse and personal to something concentrated, documented, and dangerously portable.

OLD WAY

Arrived

with a modest base of prior experience

Accumulated

know-how gradually over years of work

Departed

with a portion of what they learned - largely in their head, difficult to replicate

Leakage

was real but slow, imprecise, and hard to act on

NEW WAY

Arrived

and immediately begins encoding expertise into AI tools using company data and systems

Accumulated

know-how rapidly into structured, legible formats - prompt libraries, AI workflows, fine-tuned outputs

Departed

with a comprehensive, reproducible, immediately deployable knowledge asset

Leakage

is fast, precise, and immediately actionable by a competitor

What took years to build and was nearly impossible to steal, can now be captured, exported, and deployed in weeks.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

WHY IS THIS HAPPENING, A PERFECT STORM

SIX CONVERGING FORCES HAVE CREATED A PERFECT STORM AND MOST ORGANIZATIONS ARE CAUGHT UNPREPARED IN THE MIDDLE OF IT.

Technology has moved faster than institutions, contracts, and awareness closing that gap requires coordinated action across legal, HR, and operations.

- Know-how legibility is increasing — at employers' urging, making disagreements easier to have.
- Workers need their AI prosthesis — and they are building it right now.
- Workers are becoming managers — but now it is not "all in their head".
- Secrets intermix with general learning in files — difficult to disentangle.
- Existing contracts are either unclear or overreaching.
- Employers don't know what is unique — and the volume of items to judge is rising fast.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

THE TRANSITION STAGE IS LEAKING

The most dangerous moment is right now - employees are encoding knowledge into AI tools before any policy, agreement, or protection framework is in place.

It is happening now - we are all at a transition stage

- Know-how is becoming legible faster than legal counsel can identify what needs protecting.
- Arguments by employees claiming ownership and competitors seeking to benefit are being prepared in advance of any employer action.
- Early departures are already producing disputes over AI-encoded work product: who owns the prompts, the workflow, the output? The employee insights and mind-set?
- **The transition window is closing -** every day without a policy is a day of unprotected know-how creation.

The risks can be due to malicious acts, but most likely problems will be caused by honest or naive activities or simply confusion due to lack of framework

The clock is already running —every day without a framework is another day of unprotected, contested knowledge creation.

Critical Issue #1 Transition Stage

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

ACT NOW: FOUR IMMEDIATE ACTIONS

Four immediate actions can close the most dangerous gaps before disputes begin.

STEP 1

Audit Now

Immediate inventory of AI tool usage across all departments. Identify what is being built, by whom, and using which data sources — before any additional IP is created without a framework.

STEP 2

Interim Policy Notice

Communicate to all employees, asserting the employer's position on AI-encoded work product. A notice now — even before full agreement revision — establishes the employer's intent and limits ad hoc claims.

STEP 3

Accelerate Agreement Review

Update employment contracts to address AI tools, data use, and departure obligations. Existing agreements are silent on prompt libraries, AI workflows, and encoded know-how — close those gaps now.

STEP 4

Prioritize High-Risk Roles

Identify employees with the broadest data access and most sensitive AI workflows for immediate action. Not all roles carry equal risk — target resources where exposure is greatest.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

AGREEMENTS ARE NOT READY

Current agreements were written for a world without AI — every major worker category has unaddressed gaps.

Employees

- **No AI tool definition**
  Agreements silent on prompt libraries, AI workflows, encoded know-how
- **Custom prompt ownership**
  Unclear — company data used, but no clause addresses output rights
- **No export prohibition**
  Nothing prevents departing employees from taking AI tools
- **Personal AI accounts**
  No provisions on using personal platforms with company data

Sub-contractors

- **Weaker IP assignment**
  Freelance developers building AI tools may retain rights by default
- **Genuinely ambiguous ownership**
  When contractor uses your data to build an AI tool, who owns it?
- **No data input rules**
  No restrictions on what company data enters third-party AI platforms
- **Exit obligations absent**
  No structured handoff of AI tools or interaction history at project end

Critical Issue #2 Agreements Are Not Ready

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

CONSULTANTS

Cross-Engagement Risk

AI tools built for one client may carry encoded know-how into the next engagement — creating contamination between competing clients.

Overreaching Backfires

Claiming all AI outputs including general expertise may be unenforceable — and will deter top consultants from accepting your engagements.

Vendor AI Terms Unreviewed

The consultant's own AI platform terms may grant rights to your confidential data without your knowledge or consent.

No Audit Trail

No documentation of what data was input or what AI tools were built during the engagement — making disputes nearly impossible to resolve.

REQUIRED ACTION

All agreements must be reviewed and updated to address AI tools, data inputs, output ownership, exit obligations, and permitted personal use, across all worker categories simultaneously. Piecemeal updates leave critical gaps.

Consultants create a unique cross-client contamination risk, and most engagement letters are completely silent on it.

SAMPLE CONTRACT PROVISION: OWNERSHIP OF AI ASSETS

Ownership of AI Assets and AI Outputs

The Contractor acknowledges that, as between the parties, all right, title, and interest in and to the Client Data shall remain vested exclusively in the Client. To the extent the Contractor develops, trains, configures, customizes, fine-tunes, or otherwise creates any artificial intelligence model, system, tool, agent, workflow, prompt library, knowledge base, algorithm, or similar technology using, incorporating, derived from, or based upon Client Data (collectively, "AI Assets"), such AI Assets, together with all associated intellectual property rights therein, shall be deemed works made for hire for the benefit of the Client and, to the extent not automatically vested in the Client, are hereby irrevocably assigned to the Client. The Contractor further assigns to the Client all rights, title, and interest in and to any outputs, results, analyses, recommendations, content, software code, documentation, reports, or other materials generated by or through such AI Assets in connection with the Services ("AI Outputs").
The Contractor shall not use, commercialize, license, disclose, transfer, or otherwise exploit any AI Asset or AI Output that incorporates, is derived from, or could reasonably enable the reconstruction of Client Data or Client Confidential Information, except as expressly authorized in writing by the Client.

Carve-Out: Contractor Background Technology

Not with standing the foregoing, the Contractor shall retain ownership of its pre-existing technology, software, models, tools, methodologies, frameworks, know-how, and other intellectual property developed independently of the Services ("Background Technology"), provided that such Background Technology does not contain, incorporate, reveal, or depend upon Client Data or Client Confidential Information. The Client shall own all client-specific customizations, training results, configurations, workflows, prompt libraries, knowledge bases, and other AI Assets created specifically for the Client or developed through the use of Client Data.

Clear contractual language is available; it just needs to be added before disputes arise, not after. Of course, it reflects company (IP) policy.

Critical Issue #3 rights are intermixed

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

THE RIGHTS OF BOTH SIDES ARE INTERMIXED

AI artifacts are being created using both employee and employer input — and the contributions are not easy to separate.

Employers

- AI work uses employer's confidential information and significant resources, including compute time and working hours.
- AI artifacts would not exist without the employer's specific needs and resources.
- Employer may have a strong claim to ownership, copyright, and moral rights.
- Note: AI artifacts do not necessarily contain confidential information themselves.

Employees

- AI tools are a genuine extension of the employee — they cannot function without them and will need similar tools at their next job.
- Artifacts crystallize knowledge and insights gained over many years at previous employers.
- Employees reasonably expect to grow professionally during employment.
- AI artifacts are highly personal and may not be easily transferable to a replacement.

Solutions - not easy
Create modular artifacts; be clear about usage vs. ownership rights. Scanning for incorporated secrets may be possible using AI itself.

Critical Issue #4 The Employee - manager

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

THE EMPLOYEE AS MANAGER AND IP SOURCE - I

The employee who uses AI agents is now effectively a manager of a non-human workforce and neither employment law nor IP law has fully adapted to this reality.

Employee as Manager

- An attorney, engineer, or analyst directing AI agents to research, draft, analyze, and communicate performs a managerial function but the "team" is invisible to the organization.
- Such workers can unintentionally cause damage: there is no managerial oversight mechanism but liability exists.
- The "team" is invisible to compliance, legal, and IT operating below the organization's line of sight.
- Possible Solution
- Employees should report which AI tools they use and for what. The company should keep a simple, up to date list.

Worker Becomes an IP Source

- The employee's AI workflow is a structured accumulation of organizational intelligence, an IP asset created without a formal IP creation process or value capture.
- Every employee using AI now generates protectable IP assets, yet most organizations lack any formal IP creation process for this output.
- The company structure may not be prepared for so many simultaneous creators generating valuable assets.
- Possible Solution: State clearly that AI setups and workflows created at work belong to the company. Include this in employment contracts. AI can help record.

Every AI-empowered employee is now both a manager and an IP generator — organizations need frameworks for both realities.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

EMPLOYEE AS MANAGER AND IP SOURCE (II)

No Visibility

Legal counsel, compliance, and IT have no view into the AI agents operating under each employee's supervision, nor what data those agents access.

Solution Set up basic oversight so the company can see which AI tools are in use and what data they access. Can be automated.

Skills Are Personal - Recording Is Not Enough - new skills require new know-how

An AI tool may be documented in files, but its full value lies in the employee's ability to configure, refine, and direct it — not transferable by copying files alone.

Solution Employees in AI-heavy roles should document how they work in a way others can follow. Require proper handover before departure.

The Departure Problem

When the employee leaves, what happens to the AI agents, tool configurations, interaction history, and embedded know-how? Who inherits the "team"?

Solution Treat AI tools like any other company system —revoke or reassign access when someone leaves, require formal handover, ensure continuity.

A&I LAW FIRM

Putting It All Together

Case Study
A&I

Fictional law firm - representative of any AI-adopting organization

3	22	6
Departments	WorkersTotal	Months of AI

Staff Breakdown

- **14** attorneys +**2** interns
- **2** paralegals
- **1** marketing
- **2** accounting + **1** receptionist

After seeing this presentation, A&I contacted me for help.
They are wondering:
How long it will take or how much it will cost.

3 Departments

- Real Estate
- Litigation
- Commercial

AI Crept Into Daily Practice - 6 Months Ago Ongoing

- Letter Drafting
- Client Risk Management
- Contract Review & Clause Drafting
- Simulation of Negotiations

They should be wondering: are they are able and willing to overhaul many company procedures and relationships

FIGURE OUT WHAT MATTERS (I)

Before you can protect anything, you need to know what is actually valuable - a deliberate, cross-functional inventory is the essential first step.

Trade Secrets

What specific information - client lists, pricing models, proprietary methodologies, competitive intelligence - derives value from being kept confidential?

- Identify data that gives the organization a competitive edge and would lose value if disclosed
- Map where this information currently resides - and whether AI tools have already encoded it

> In A&I
> Pricing structures and key client relationships are the primary trade secrets to protect

Know-How Creation

Where in the organization is expertise being actively encoded into AI tools? Which roles, departments, and workflows are generating AI-embedded know-how right now?

- Survey all departments for active AI tool usage - prompt libraries, workflow automations, fine-tuned outputs.
- Do not assume the most senior employees are the biggest risk - junior staff may be the most active AI builders

> In A&I
> Interns, paralegals, and non-legal staff may have the most time and need —and therefore the most active AI encoding activity

FIGURE OUT WHAT MATTERS (II)

Before you can protect anything, you need to know what is actually valuable - a deliberate, cross-functional inventory is the essential first step.

Competitive Advantages

What capabilities, if replicated by a competitor, would genuinely harm the business? These are priority protection targets.

A&I: How does A&I make their money? Do they have a key differentiator?

Worker Expectation

What do employees believe they own? Misaligned expectations are the source of future disputes — understanding them now reduces later conflict.

A&I: Lawyers expect employment flexibility and the ability to open their own firms.

Executive Attitude

What is leadership's appetite for enforcement vs. flexibility? Policy must be realistic to be implementable.

A&I: Managing partner may believe in a "take it or leave it" approach.

IDENTIFY TOUCH POINTS / VULNERABILITIES (PART I)

Contracts

Employment, contractor, and consulting arrangements — formal legal interfaces where AI ownership must be explicitly defined.

Within the Company

Teams sharing AI tools or training others on workflows create shared ownership complexity and potential information leakage across departments.

In A&I: Did A&I commit to special secrecy to one client? Internal AI-sharing may breach that commitment.

Problematic Positions

Partners,seniorengineers,keyaccount managers — those with the broadest data access and most sensitive client relationships pose the greatest leakage risk.

In A&I: A junior associate who is deeply into AI tooling — broad access, high enthusiasm, no formal ownership framework yet in place.

Every knowledge transfer point is a potential vulnerability. Map them all before designing protections.

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

IDENTIFY TOUCH POINTS / VULNERABILITIES (PART II)

High Churn Roles

High-turn over positions are high-risk transfer points - every departure is a potential leakage event.

Uncertain Relationships

New hires, interns, freelancers, contractors ownership rules not yet clearly established.

In A&I: In A&I: New associates come with different AI default habits.

Between Companies

Joint ventures, partnerships, outsourced functions — AI tools built collaboratively may have disputed ownership. Look at relationships between and within the company - where knowledge flows.

In A&I: A junior associate who is deeply into AI tooling — broad access, high enthusiasm, no formal ownership framework yet in place.

Independent Contractors

Weaker default IP assignment rules explicit contractual language is essential.

In A&I: Does A&I work with external experts?

High-churn roles and cross-company relationships are the most overlooked vulnerability points —don't underestimate either.

SET POLICY (I)

Policy is not a document. It is a set of clear decisions about where the line is, what employees are free to keep, and what the organization must protect.

Agreement Review Standard

All existing agreements reviewed against new policy; new agreements incorporate updated language as baseline. Don't forget partnership agreements too.

AI Tool / Scenario	Owner	Rationale
Legal research workflows built on firm data	Company	Proprietary data and know-how embedded
AI tools built by contractors / interns	Company	Requires explicit contract clause

Establish the Line

AI tools built using company data, systems, or time = company property.
Personal workflows using only public knowledge may be retained.

Classification Principle	Owner	Note
Company data / systems / time used	Non-Negotiable	Core ownership rule applies to all worker categories
Public knowledge, personal time only	Employee	Employee may retain reduces exit conflict

SET POLICY (II) - WHAT EMPLOYEES MAY KEEP & WHAT MUST STAY

Identify Freebies — Decide What Departing Employees May Keep

AI Asset / Workflow Type	Owner	Rationale
General-purpose AI skill set (public data only) Workflows built exclusively on publicly available knowledge — no client or company data embedded	Employee — Negotiable	Freebie - reduces exit conflict and aids talent retention
Agreement templates & clause libraries AI-curated template sets and standard clause databases	Company — Review	Depends on data source used to build the library

Secrecy — Client Data, Methodologies & Trade Secrets Must Stay

AI Asset / Workflow Type	Owner	Rationale
Personal AI accounts used with company data Employees' private platform accounts where company or client data was input during work	Restricted — Review	Policy must define permitted use; data inputs create confidentiality risk
Client-specific AI tool configurations Models, agents, prompt libraries built with or around specific client data and relationships	Company — Non-Negotiable	Contains confidential client information — non-negotiable

Defining "freebies" upfront is not generosity — it is a strategic tool for reducing exit conflict and retaining top talent.

IMPLEMENT (I)

Policy without implementation is decoration - the gap between what the agreement says and what employees actually do is where IP is lost.

Contracts:

Existing Agreements: Audit all current contracts and issue updated agenda addressing AI tools, data use, and departure obligations

A&I expects conflict, but better now than later

Going forward: All new hires, contractors, and consultants onboard with AI-aware agreement language from day one

Educations:

Identify targets: Prioritize training for high-risk roles - senior professionals with access to sensitive data and AI tools In A&I, non-AI partners need to understand issues

Train employees: What they can and cannot do with AI tools, permitted data inputs, and obligations upon departure A&I prepared a booklet with examples

Contracts set the rules; education makes them real —both are required for the framework to hold.

MAINTAIN AND ADAPT - I

This is not a one-time project - AI technology, employee practices, and the legal landscape are all changing rapidly, and your framework must change with them.

- Knowledge management role: Designate someone accountable for tracking how AI tools are built, updated, and used across the organization
  - In A&I, a senior associate with an attraction to AI is also in charge of AI assimilation and risk detection
- Regular policy review: Schedule periodic reviews at minimum annually as AI capabilities, employee practices, and legal standards evolve
  - In A&I the AI-associate creates a report for the management team and meets quarterly to raise AI-related issues
- Technology changes: New AI platforms and agent capabilities create new touch points; the audit and policy-setting process must repeat as technology evolves
  - The AI-associate must vet any platform use and actively discuss new abilities with users
- Legal landscape evolving: Courts are actively resolving AI copyright, trade secret, and employment cases in 2025–2026; monitor decisions and update policies accordingly
  - In A&I the AI associate has background in IP & employment law
- Adapt, don't just enforce: The goal is a living framework that protects organizational interests while remaining attractive to the talent needed to stay competitive

EHRLICHGROUP
TURNING IDEAS INTO VALUE SINCE 1995

ADV. YEHUDA NEUBAUER

MAIER FENSTER

Putting It All Together

CONCLUSIONS

AI is fundamentally **changing** how organizational knowledge is created, captured, managed, and protected.

Know-how is no longer locked in people's minds. It is becoming **structured**, **portable**, and **reusable**.

Most organizations still have **no clear framework** defining ownership of AI-generated assets.

Contracts, policies, onboarding, and offboarding processes must **evolve** to address AI.

AI governance is not about restricting innovation. It is about **protecting the business** while enabling responsible adoption.

Balance protection with **flexibility**. Overreaching policies may discourage the very talent you want to attract.

Treat AI workflows, prompt libraries, and agent configurations as **valuable business assets**.

The transition is **happening now**. Every day without a framework increases the risk of unnecessary disputes, trade secret leakage, and AI-mediated business damage.

> "The question is no longer whether your employees use AI to make know-how more legible.
> **The question is whether your organization is prepared for the consequences.**"

TAKE A PHOTO.
SAVE THE KEY POINTS.
SHARE WITH YOUR TEAM.

Thanks

And See You Next Time

MAIER FENSTER

ADV. YEHUDA NEUBAUER