WHY COMPANIES NEED A PRIVATE AI WORKSPACE BEFORE SENSITIVE DATA LEAVES THE ORGANIZATION

Prepared by cogify

Featuring IVY-powered Private AI Workspace Implementation, Maintenance and Cybersecurity Consulting

COGIFY

EXECUTIVE SUMMARY

Artificial intelligence is already part of everyday work.

Employees use public AI tools to summarize documents, rewrite emails, translate content, prepare presentations, analyze reports, support sales, review contracts, write code and speed up repetitive tasks. This is not automatically a problem. AI can improve productivity, reduce manual work and help teams move faster.

The problem starts when companies do not know which AI tools employees are using, what data is being entered, where that data is processed, whether access rights are respected and whether **company security rules** are followed.

This unmanaged use of AI is often called **shadow AI**.

Shadow AI creates a **cybersecurity and data protection risk** because sensitive company information can leave the organization through simple employee behaviour: copying documents into public AI tools, uploading files for summarization, pasting source code into chatbots or asking AI to rewrite **confidential client content**.

For technical teams, the risk can be even more serious. Developers and IT employees may paste error logs, API keys, access tokens, environment variables, database details, system architecture, technical **usernames and passwords** into public AI tools while trying to debug, document or understand a problem faster.

This is usually not caused by bad intention. Employees are trying to be efficient. But from a cybersecurity perspective, the result can still be **serious data exposure**.

The solution is not to ban AI completely. Employees use AI because it helps them work faster. If companies do not provide a safe and useful alternative, employees may continue using public tools through personal accounts, browser tools, mobile apps or unmanaged workflows.
A better approach is **secure AI adoption** through a private AI workspace.

cogify helps companies implement, operate and maintain a private AI workspace where employees can use AI for company knowledge, document search, summarization and daily work without sending sensitive information into public AI tools. The workspace can be powered by IVY, cogify's private AI technology layer. The client-facing solution is simple: a **private AI workspace** where company data stays inside the company, in a controlled environment.

This environment can be hosted on cogify's **Swiss infrastructure** or installed in the **client's own server** or private environment, depending on the client's security, data protection and operational needs.

Inside the workspace, company data is controlled through **separate workspaces**, role-based access rights, approved knowledge sources and clear restrictions. **Employees access** only the information they are allowed to see.

HR documents can be restricted to HR. Finance documents can be restricted to finance and management. Client project data can be separated per client or project team. Technical documentation can be limited to developers and IT. Board and strategy documents can be limited to leadership.

This gives companies a practical alternative to uncontrolled public AI use. **Employees get AI for daily work.**

Management keeps control over data, access rights, hosting and cybersecurity risk. Company knowledge stays inside a controlled company environment, ensuring data never leaves the company.

TABLE OF CONTENTS

Pages	
1	1. The New Reality: AI Is Already Inside the Workplace
2	2. What Is Shadow AI?
3	3. Why Shadow AI Is a Cybersecurity Issue
5	4. Warning Signs From the Market
6	5. Swiss Context: Why Shadow AI Matters for Swiss Companies
7	6. Practical Swiss Risk Scenarios
10	7. Why “Just Ban AI” Is Not Enough
11	8. What Companies Need Instead
12	9. How Data Is Controlled Inside the Company
15	10. How cogify Helps
17	11. AI Security Checklist for Management
18	12. Recommended First Steps
19	Conclusion
20	References & Further Reading

1. THE NEW REALITY: AI IS ALREADY INSIDE THE WORKPLACE

AI IS NO LONGER A FUTURE TREND. IT IS ALREADY PART OF DAILY BUSINESS.

Employees use AI tools to summarize reports, rewrite emails, draft offers, translate documents, analyze spreadsheets, review contracts, explain technical content, debug code, prepare customer responses, create meeting notes and improve marketing or sales content.

Most employees do this with good intentions. They are not trying to harm the company. They are trying to save time, improve quality and keep up with expectations.

But from a cybersecurity perspective, unmanaged AI use creates a serious blind spot.

A company may not know:

- which AI tools are being used
- whether employees use personal or company accounts
- whether confidential documents are pasted into public tools
- whether customer or employee data is being shared
- whether source code, credentials or technical architecture are exposed
- where AI prompts and uploaded files are stored
- whether access rights are respected
- whether AI-generated answers are accurate or safe
- whether AI use is aligned with internal policies

The core challenge is simple:

Productivity is moving faster than governance.

2. WHAT IS SHADOW AI?

Shadow AI is the use of artificial intelligence tools inside an organization without proper approval, governance, visibility or control from IT, security or management.

It is similar to shadow IT, where employees use unapproved tools or cloud services to get work done faster. But shadow AI can be more sensitive because AI tools do not only store data. They process, summarize, rewrite, infer and generate new outputs from the information employees provide.

That means a simple copy-paste action can expose information that would normally be protected inside company systems.

SENSITIVE INFORMATION THAT MAY ENTER UNMANAGED AI TOOLS INCLUDES:

- customer documents
- contracts and legal files
- internal reports
- board material
- source code
- API keys and access tokens
- technical usernames and passwords
- database credentials
- environment variables
- error logs and system traces
- internal URLs
- server and cloud configuration details
- employee information
- HR documents
- financial data
- sales pipelines
- product roadmaps
- business strategy
- support tickets
- security procedures
- client communication
- project documentation
- supplier information
- public-sector-related documents

In many cases, this information is not exposed through a cyberattack. It is exposed through everyday employee behaviour.

A person wants a faster summary. A manager wants a cleaner email. A developer wants help with code. A salesperson wants to rewrite a proposal. A finance employee wants help explaining a spreadsheet.
The intention is productivity.

The result can still be data exposure.

3. WHY SHADOW AI IS A CYBERSECURITY ISSUE

Shadow AI should not be treated only as an innovation topic. It is also a cybersecurity issue. Traditional cybersecurity protects systems, files, access rights, emails, networks and devices. But public AI tools create a new path for sensitive information to leave the company.

A confidential document may be protected in the company's internal system. But if an employee copies the content into an external AI tool, the original access control no longer matters.

Shadow AI creates several risks.

DATA LEAKAGE

Confidential business data may be shared with a tool that is not approved, monitored or contractually controlled by the company.

LOSS OF VISIBILITY

IT and security teams may not know what data was shared, by whom, with which tool and for what purpose.

LOSS OF ACCESS CONTROL

Information from restricted documents can be copied into an AI chat and then shared with people who should not have access to the original content.

COMPLIANCE AND DATA PROTECTION RISK

Personal data, customer data, employee data or regulated information may be processed outside approved environments.

INTELLECTUAL PROPERTY EXPOSURE

Source code, technical architecture, product ideas, research, proprietary algorithms and business know-how may be exposed through prompts or uploaded files.

UNRELIABLE OUTPUTS

AI-generated answers may look professional but contain errors, unsupported claims, insecure code or wrong assumptions.

EXPANDED ATTACK SURFACE

AI-powered workflows, chatbots and agents can be manipulated if they are connected to sensitive actions without proper verification, access control, auditability and human oversight.

CREDENTIAL AND INFRASTRUCTURE EXPOSURE

Employees may accidentally paste technical usernames, passwords, API keys, access tokens, database credentials, environment variables, server logs, internal URLs, cloud configuration details or system architecture into public AI tools.

This is especially dangerous because technical information can be directly useful to attackers. Even a short log file or error message may reveal credentials, tokens, system names, endpoint URLs, database paths or details about how a company's systems are built and accessed.

4. WARNING SIGNS FROM THE MARKET

The purpose of market examples is not to claim that every AI incident is the same. Some are employee-driven data exposure cases. Some are AI workflow exploitation cases. Some are broader AI security concerns.

Together, they show one clear lesson:

Companies need governance, security and controlled environments for AI use.

Enterprise examples have shown that employees may enter sensitive internal information, including source code, into public AI tools. Public-sector examples have shown that even security-aware environments can struggle when sensitive documents are uploaded into public AI platforms. AI-powered workflows have also shown that automation connected to sensitive actions must be designed with strong verification, access control and oversight.

The lesson is not that companies should avoid AI.

The lesson is that AI must be introduced securely.

Companies need clear rules, approved tools, controlled access rights, secure hosting models, employee guidance and ongoing review. Without this, AI adoption happens informally, and sensitive data may leave the organization before management knows there is a problem.

5. SWISS CONTEXT: WHY SHADOW AI MATTERS FOR SWISS COMPANIES

There are currently no widely confirmed public Swiss cases where a company was hacked specifically because employees overused AI tools.

However, Switzerland already has a real cybersecurity risk environment. Swiss organizations face ransomware, phishing, data extortion, software vulnerabilities, supply-chain attacks and data leakage risks.

The Xplain case also showed how serious data exposure can become when sensitive information connected to public authorities and suppliers is leaked. This was not an AI incident, but it is a strong Swiss reminder that data exposure, supplier risk and weak control over sensitive information can have significant consequences.

Shadow AI should therefore be understood as an additional risk layer.

It does not replace traditional cybersecurity risks.
It creates a new way for sensitive information to leave the organization through everyday employee behaviour:

- ⚠ copy-pasting documents into public AI tools
- ⚠ uploading files for summarization
- ⚠ translating confidential content
- ⚠ asking AI to analyze client data
- ⚠ using AI to review source code
- ⚠ pasting financial data into chat prompts
- ⚠ pasting usernames, passwords, tokens or API keys into prompts
- ⚠ generating outputs from restricted internal information

For Swiss SMEs, fiduciaries, associations, software companies, healthcare-related organizations, public-sector suppliers and consulting firms, this matters because many teams work with sensitive information every day.

A private AI workspace helps companies give employees a safer alternative to unmanaged public AI tools while keeping company knowledge, access rights and data residency under better control.

6. PRACTICAL SWISS RISK SCENARIOS

The following scenarios are not presented as confirmed Swiss AI-caused hacking incidents. They show how shadow AI risk can appear in common Swiss business environments.

FIDUCIARY OR ACCOUNTING FIRM

A fiduciary team may use AI to summarize client documents, draft emails, explain finance-related information or prepare internal notes.

Without a controlled AI workspace, employees may paste client financial documents, payroll information, tax material, invoices or personally identifiable information into public AI tools.

A private AI workspace can separate general company knowledge, client documents, payroll content, tax documents and management information into restricted workspaces. Users only receive access to the workspaces that match their role and responsibility.

For stricter client confidentiality requirements, the workspace can be installed on the firm's own servers or private environment.

SWISS SME WITH CUSTOMER PROJECTS

A Swiss service company may use AI to draft customer emails, summarize project documents, prepare offers and translate internal content.

The risk is that customer names, pricing, contractual details, project risks and internal strategy are copied into unmanaged AI tools.

A private AI workspace can be separated by department, client, project or sensitivity level. Sales can work with approved proposal material. Project teams can work with their own client documents. Management can keep strategy, pricing and board-level documents restricted.

This gives employees a useful AI workspace without opening access to all company information.

SOFTWARE OR TECHNOLOGY COMPANY

Developers and technical teams may use public AI tools to debug code, explain errors, review architecture, write documentation, generate test cases or understand system behaviour faster.

This can expose source code, system architecture, API structures, logs, usernames, passwords, API keys, tokens, database credentials, environment variables, internal URLs, cloud configuration or CI/CD information.

In software and technology companies, shadow AI can therefore become more than a documentation risk. It can become an infrastructure, access and intellectual property risk.

A private AI workspace can provide developers with approved technical documentation, architecture knowledge, onboarding material, coding standards and internal support content.

Access can be limited by role, team or project. A developer working on one product does not automatically need access to all client environments or all architecture documents.

Passwords, API keys, production credentials and access tokens should remain in approved password managers, vaults or secret-management systems. The AI workspace can support technical work, but it should not replace secure credential management.

ASSOCIATION OR NON-PROFIT ORGANIZATION

An association may handle member records, supplier invoices, board documents, event participant lists and administrative files.

Employees may use public AI tools to summarize meeting notes, translate member communication or rewrite board documents.

A private AI workspace can divide information into general administration, member communication, finance, board and event workspaces. Board documents can stay restricted to board members. Finance data can stay restricted to finance and authorized management. Event documents can be available only to the people organizing the event.

This helps small teams benefit from AI without mixing all documents into one open environment.

PUBLIC-SECTOR SUPPLIER OR AUTHORITY-RELATED ORGANIZATION

Swiss organizations working with public authorities often handle contracts, project documentation, citizen-related information, technical documents or operational data.

This information may not always be classified, but it may still be sensitive, contractually protected, reputationally important or security-relevant.

A private AI workspace can be structured by authority, client, project, contract or sensitivity level. This reduces the risk that authority-related data is mixed with general company content or made available to users who do not need it.

For authority-related or highly sensitive work, the workspace can be installed on the client's own servers or private infrastructure.

HR, RECRUITMENT OR HEALTHCARE-RELATED ORGANIZATION

Teams working with health-related, HR or recruitment information may use AI to summarize CVs, write employee communication, prepare reports or structure interview notes.

These workflows can involve personal data, sensitive employee information or confidential assessments.

A private AI workspace can separate general HR knowledge, recruitment material, employee documentation, management content and onboarding policies.

Recruiters may access candidate-related material. HR may access employee policy and process documentation. Management may access restricted decision documents. General employees may only access approved HR policies, onboarding guides or internal FAQs.

The goal is not to automate sensitive human decisions. The goal is to support safe knowledge work while keeping personal and internal information out of unmanaged AI tools.

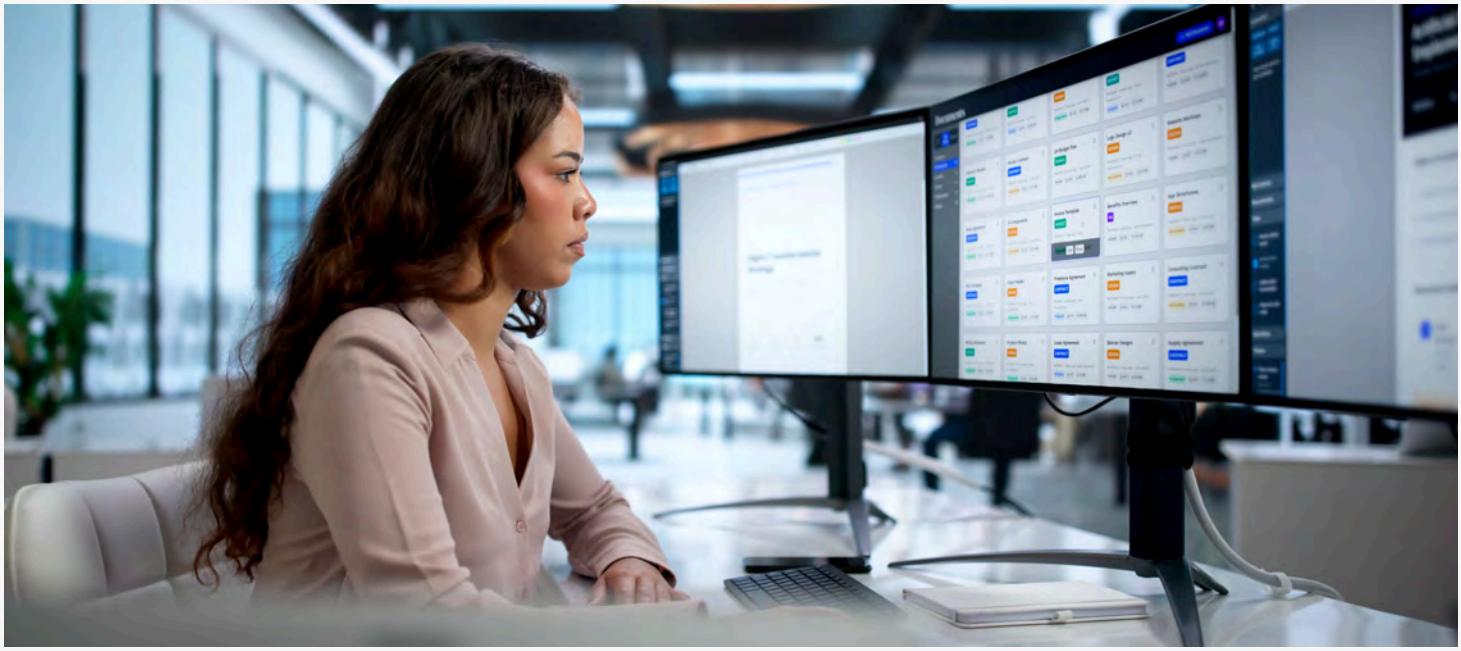
7. WHY “JUST BAN AI” IS NOT ENOUGH

Some organizations try to reduce risk by banning public AI tools.

This may be necessary in some cases, but it is usually not enough as a long-term strategy.

Employees use AI because it helps them work faster, save time, reduce repetitive tasks, improve writing quality, understand complex information and stay competitive.

If the company does not provide a safe and useful alternative, employees may continue using AI through personal accounts, browser tools, mobile apps or unmanaged platforms.



A full ban can create a false sense of security. Management may believe AI use is controlled, while employees continue using external tools quietly.

A better approach is secure AI adoption.

This means giving employees a company-approved AI environment with clear rules, controlled knowledge sources, access rights and cybersecurity support.

The goal is not to stop people from using AI.

The goal is to give them a safer place to use it.

8. WHAT COMPANIES NEED INSTEAD

The challenge with public AI tools is simple:
Employees often copy company information into systems the company does not control. cogify helps companies solve this by implementing a private AI workspace where sensitive company data does not need to leave the controlled company environment.

The workspace can be powered by IVY, cogify's private AI technology layer. The solution is not positioned as selling an AI model. The solution is a secure private workspace that employees can actually use in daily work.

A private AI workspace can support:

- company knowledge search
- document summarization
- internal Q&A
- drafting of emails, reports, proposals and presentations
- meeting notes and business documentation
- technical documentation support
- onboarding and internal knowledge sharing
- controlled AI-assisted work across departments

The workspace is designed around the client's real environment:

- their documents
- their knowledge sources
- their access rights
- their security requirements
- their infrastructure
- their internal rules
- their data protection needs

Depending on the client's requirements, the private AI workspace can be:

- hosted on cogify's Swiss infrastructure
- installed on the client's own servers
- deployed in a private environment defined together with the client

The result is simple: **Employees get AI for daily work.** Company knowledge stays under company control.

Sensitive data does not need to leave the company environment. Management gains a safer and more governable alternative to public AI tools.

9. HOW DATA IS CONTROLLED INSIDE THE COMPANY

A private AI workspace is only useful if the company can control which information is available, who can access it and where the data is processed. This is why the workspace must be designed with restrictions from the beginning.

CONTROLLED HOSTING OR CLIENT-SIDE DEPLOYMENT

The private AI workspace can run on cogify's Swiss infrastructure or inside the client's own server or private environment. This means company documents, prompts, knowledge sources and AI-assisted workflows do not need to be sent into public AI tools.

The deployment model is selected based on the client's requirements:

- Swiss hosting operated by cogify
- installation on the client's own servers
- deployment in a private environment
- restricted setup for sensitive sectors or authority-related work

The goal is to keep company data inside a controlled environment instead of spreading it across unmanaged public AI accounts.

SEPARATE WORKSPACES

A private AI workspace should not be one open space for all company data. It should be structured into separate workspaces based on the company's organization, sensitivity levels and real working processes.

Examples include:

- General Company Workspace
- HR Workspace
- Finance Workspace
- Sales Workspace
- Client Project Workspace
- Development Workspace
- Internal IT Workspace
- Management Workspace
- Board Workspace
- Public-Sector or Authority-Related Workspace

Each workspace can have its own approved documents, users and access rules. This prevents sensitive information from being mixed with general knowledge.

ROLE-BASED ACCESS RIGHTS

Access to each workspace should be based on the user's role and business need.

For example:

- all employees may access company policies and approved internal FAQs
- HR may access HR processes, employee templates and recruitment material
- finance may access finance procedures and invoicing documentation
- developers may access technical documentation and coding standards
- project teams may access only their own client project workspace
- management may access strategy, board and restricted decision documents
- board members may access only board-approved materials

The principle is simple:

Employees should only see what they are allowed to see. AI should not become a shortcut around existing access rights.

APPROVED KNOWLEDGE SOURCES

The private AI workspace should only use approved company knowledge sources.

Before documents are connected, the company should decide which documents:

- are safe to use
- are restricted
- require review
- should be excluded
- must be anonymized or cleaned
- contain personal data
- contain technical secrets
- belong to a specific client or project

This keeps the AI workspace aligned with the company's internal rules.

PERMISSION-AWARE ANSWERS

The workspace should respect access rights when generating answers.

A user should only receive answers based on documents and knowledge sources they are allowed to access.

For example:

- marketing should not receive answers based on HR salary documents
- developers should not receive answers based on board strategy documents
- one project team should not receive answers based on another client's restricted files
- general employees should not receive answers based on finance or legal documents

This is one of the most important differences between a controlled private AI workspace and unmanaged public AI use. Public AI tools do not know the company's access rights. A private AI workspace can be structured around them.

TECHNICAL SECRETS AND CREDENTIALS

Technical secrets require special handling.

A private AI workspace should not become a place where passwords, API keys, production credentials or access tokens are stored without control. These should remain in approved password managers, vaults or secret-management systems.

For development and IT teams, the company should define clear rules:

DON'T:

- paste passwords into AI prompts
- paste API keys into AI prompts
- paste production credentials into AI prompts
- upload unreviewed logs that may contain secrets
- upload environment files without review

DO:

- sanitize technical documentation before connecting it to the workspace
- keep secrets in dedicated secret-management tools

The AI workspace can support technical work, but it should not replace secure credential management.

10. HOW COGIFY HELPS

cogify helps companies adopt AI safely by combining private AI workspace implementation, cybersecurity consulting, Swiss hosting and long-term technical support.

PRIVATE AI WORKSPACE IMPLEMENTATION

cogify designs and implements a private AI workspace based on the client's business needs, data sensitivity, infrastructure and security requirements.

The workspace can be powered by IVY, cogify's private AI technology layer.

This includes setup, configuration, knowledge-source connection, workspace structure, access-right logic and deployment planning.

SECURE HOSTING OR CLIENT-SIDE DEPLOYMENT

The private AI workspace can be hosted on cogify's Swiss infrastructure or installed in the client's own server or private environment.

The right deployment model is selected based on the client's data protection, cybersecurity, compliance and operational requirements.

WORKSPACE AND ACCESS-RIGHT DESIGN

cogify helps clients define how data should be separated inside the workspace.

This includes department workspaces, project workspaces, client-specific workspaces, management workspaces and restricted workspaces for sensitive content.

The goal is to make sure users only access the information they are allowed to use.

iVY

CYBERSECURITY CONSULTING

cogify helps companies reduce shadow AI risk through cybersecurity consulting, access review, sensitive data mapping, policy support, employee guidance and AI workflow security review.

This includes rules for confidential data, client information, HR data, financial data, source code, credentials, logs and technical secrets.

MAINTENANCE AND CONTINUOUS IMPROVEMENT

Secure AI adoption does not end after the initial installation.

cogify can support the ongoing operation of the private AI workspace through:

- technical updates
- security updates
- access-right adjustments
- support for new users or departments
- review of connected knowledge sources
- improvement of document structure
- review of user feedback
- optimization of AI workflows
- periodic cybersecurity review

This is important because AI use cases evolve quickly. New departments request access, new documents are created, new risks appear and internal policies change.

With ongoing support, the workspace remains useful, secure and aligned with business reality.

11. AI SECURITY CHECKLIST FOR MANAGEMENT

Companies should ask:

- Do we know which AI tools employees use?
- Are employees using personal AI accounts for work?
- Do we know what data is being pasted into AI prompts?
- Do we have rules for client data, HR data, financial data and source code?
- Do we have rules for usernames, passwords, API keys, tokens and logs?
- Do we have an approved AI workspace?
- Is the workspace separated into restricted areas?
- Are company knowledge sources controlled by access rights?
- Can users only access workspaces relevant to their role?
- Do we know where AI-related data is hosted?
- Do we train employees on safe AI usage?
- Do we monitor and review AI risks regularly?
- Are AI-generated outputs reviewed before being used in sensitive workflows?
- Do we know which AI tools are connected to company systems?
- Do we have clear ownership for AI governance?
- Do we have maintenance and support for our AI workspace?

If the answer is “no” to several of these questions, the company may already have shadow AI risk.

12. RECOMMENDED FIRST STEPS

For companies concerned about shadow AI, cogify recommends the following first steps.

STEP 1: IDENTIFY CURRENT AI USAGE

Understand which AI tools employees already use, which departments use them and for what purpose.

STEP 2: CLASSIFY SENSITIVE DATA

Define which data should never be entered into public or unmanaged AI tools.

This should include client data, employee data, financial data, source code, credentials, usernames, passwords, API keys, access tokens, logs and technical configuration details.

STEP 3: REVIEW ACCESS RIGHTS

Check who should be able to access which internal knowledge sources.

STEP 4: DESIGN WORKSPACE RESTRICTIONS

Define which workspaces are needed. For example:

- general company workspace
- HR workspace
- finance workspace
- development workspace
- client project workspace
- management workspace
- board workspace

For each workspace, define who can access it, which documents are included and which data must remain restricted.

STEP 5: CHOOSE THE RIGHT DEPLOYMENT MODEL

Decide whether the private AI workspace should run on cogify's Swiss infrastructure, inside the client's own servers or in another private environment.

STEP 6: IMPLEMENT, TRAIN AND GOVERN

Set up the workspace, connect approved knowledge sources, configure access rights, train users and create governance rules around AI usage.

STEP 7: MAINTAIN AND IMPROVE CONTINUOUSLY

Review usage, improve knowledge sources, update access rights, support employees and adapt the workspace as business and security needs evolve.

CONCLUSION

AI is already inside the workplace. The question is no longer whether employees will use AI, but whether the company can provide a safe and controlled environment for it. Unmanaged AI use creates cybersecurity, data protection and compliance risks. Banning AI alone is not a realistic long-term solution.

Companies need secure AI adoption. cogify helps companies implement, operate and maintain private AI workspaces that support real daily work while reducing reliance on unmanaged public AI tools. The workspace can be powered by IVY, cogify's private AI technology layer. The client-facing solution is simple: a private AI workspace where data does not need to leave the controlled company environment.

Company information can be separated into restricted workspaces. Access can be defined by role, department, project or sensitivity level. HR documents can stay with HR. Finance documents can stay with finance. Client data can stay inside client-specific workspaces. Technical documentation can stay with authorized developers and IT. Management and board material can stay restricted to leadership This is how companies can give employees AI without losing control over company knowledge.

Combined with cybersecurity consulting, governance support and long-term maintenance, a private AI workspace gives organizations a practical way to reduce shadow AI risk, protect sensitive information and build a stronger foundation for responsible AI use.

READY TO GIVE EMPLOYEES AI WITHOUT LOSING CONTROL OF COMPANY DATA?

Talk to cogify about private AI workspace implementation, maintenance and cybersecurity consulting.

We help you understand how employees may be using AI today, where sensitive information could be exposed and how a private AI workspace can give your company a safer alternative to public AI tools.

Request an AI Security Consultation

IMPORTANT DISCLAIMER

The Swiss use cases in this white paper are practical business scenarios based on common workflows in Swiss SMEs, fiduciaries, associations, technology companies, healthcare-related organizations and public-sector-related environments.

They are not presented as confirmed Swiss AI-caused hacking incidents.

The confirmed Swiss references are used to demonstrate the broader cybersecurity environment in Switzerland, especially data exposure, ransomware, phishing, supply-chain and governance risks. Shadow AI should be understood as a new risk layer that can increase data exposure if companies do not provide secure, approved AI workflows.

The deployment model for a private AI workspace should be defined based on each client's security, data protection, compliance and operational requirements. For some clients, cogify-operated Swiss infrastructure may be suitable. For others, installation on the client's own servers or private environment may be preferred.

REFERENCES AND FURTHER READING

1. SWISS NATIONAL CYBER SECURITY CENTRE: SEMI-ANNUAL REPORT 2025/1

The NCSC reported 35,727 cyberincident reports in the first half of 2025 and highlighted ransomware, data extortion, phishing, DDoS attacks, software vulnerabilities and supply-chain attacks as relevant cyberthreats for Switzerland.

Link: https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2025-1.html

2. SWISS NATIONAL CYBER SECURITY CENTRE: DATA ANALYSIS REPORT OF THE HACKER ATTACK ON XPLAIN

The NCSC report explains its analysis of data published on the darknet after the hacker attack on Xplain, a major provider of IT services to national and cantonal authorities.
This is not an AI incident, but it is a relevant Swiss example of why sensitive data exposure, supplier risk and third-party technology environments matter.

Link: https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/fachberichte/bericht-datenanalyse-xplain.html

3. OWASP TOP 10 FOR LARGE LANGUAGE MODEL APPLICATIONS

OWASP's GenAI Security Project identifies and documents security and safety risks associated with generative AI technologies, including large language models and AI-driven applications.
Relevant risks include prompt injection, sensitive information disclosure, insecure output handling and excessive agency.

Link: https://owasp.org/www-project-top-10-for-large-language-model-applications/

4. CISA PUBLIC CHATGPT DOCUMENT UPLOAD CASE

ITPro reported that the acting head of the U.S. Cybersecurity and Infrastructure Security Agency uploaded sensitive "For Official Use Only" documents to a public version of ChatGPT, raising concerns around shadow AI and data control.

Link: https://www.itpro.com/security/data-protection/cisas-interim-chief-uploaded-sensitive-documents-to-a-public-version-of-chatgpt-security-experts-explain-why-you-should-never-do-that

5. SWISS FEDERAL COUNCIL: SWISS AI REGULATORY DIRECTION

The Federal Council announced that Switzerland intends to ratify the Council of Europe AI Convention and implement it through a sector-specific approach, supported by non-legally binding measures where appropriate.

Link: https://www.admin.ch/en/nsb?id=104110

AI IS USEFUL. UNCONTROLLED AI IS RISKY.

cogify helps companies move from shadow AI to secure AI adoption through private AI workspace implementation, cybersecurity consulting, maintenance and long-term technical support.

Employees can use AI for real work.

Company knowledge stays inside a controlled environment.

Data is separated through restricted workspaces.

Management keeps stronger control over access rights, data location and cybersecurity risk.