



AI Adoption Report

Shadow workforce, untapped potential,
and rules being written

Foreword:

AI ADOPTION REPORT

Artificial intelligence has quickly become an integral part of everyday work life: 87 percent of the workforce uses it at least several times a week, and nearly half use it daily. What is remarkable here is not so much the speed of this development as the question of how differently companies are dealing with it.

Recent security analyses show how real the associated risk already is: Compromised or malicious AI services and intermediary LLM routers can read and misuse not only inputs and files but also SSH keys, cloud credentials, and other digital access keys. Anyone who relies on untrustworthy providers or unregulated intermediaries therefore risks not only abstract data protection violations, but also the leakage of sensitive company information and unauthorized access to their own systems—which could even lead to criminal misuse. This isn't a threat for the future—it's a real danger right here and now.

However, this use is not in itself a sign of carelessness. It is also the result of a lack of alternatives or concrete barriers. When secure access points are lacking, employees fill the gap themselves. If compliance or data protection concerns take precedence, company-wide implementation will be delayed. This also explains why data protection and compliance—at 50 percent—are the most common reasons for ruling out an AI application. It is not the technology that is the obstacle, but rather uncertainty about the appropriate framework.

This is exactly where our approach to corporate security comes in: Using AI safely does not mean putting the brakes on innovation. The goal is to provide a reliable framework. Companies that take this approach early on not only gain a security advantage but also a tangible productivity advantage. Because our study shows: Even among experienced users, too much of AI's potential remains untapped.

That's exactly what we wanted to understand better at Myra Security. In collaboration with the polling firm Civey, we therefore surveyed 4,000 working adults to find out how, where, and when they come into contact with AI. The goal of the study was to paint a realistic picture of how AI is actually used in German companies. The result: AI is used extensively and as a matter of course—though often through channels that lie outside a company's own organizational structures. 41 percent use their personal accounts for work-related tasks. In contrast, only 33 percent use a tool provided by their employer. At the same time, sensitive content has long been ending up in precisely these applications.



Sascha Schumann
Managing Director
Myra Security GmbH

Executive Summary

Intelligent systems are already deeply embedded in our everyday work lives: 46 percent use AI daily, and 87 percent use it at least several times a week. Therefore, the question is no longer whether AI is used at all, but rather how, through which channels, and above all, with what data.

The most common access method is striking: At 41 percent, more employees use a personal account than a solution provided by their employer. A significant portion of AI use in the workplace thus takes place outside of controlled structures, as “shadow AI.” This is not without consequences, as AI has long been used to process sensitive content: 30 percent have used AI to process contracts or strategic information, 25 percent have used it to process personal data, and 15 percent have used it to process explicitly confidential data. As this type of interaction increases at higher levels of management, the most intensive use and the most sensitive data converge precisely where the need for protection is greatest.

Despite widespread use, potential remains untapped: 92 percent complete tasks without AI, even though it could have provided support, across all levels, sizes, and industries. The explanation points to the main obstacle: uncertainty regarding data protection and compliance. As a result, 50 percent have already opted out of AI or stopped using it.

And so we’ve come full circle. The main bottleneck is not a matter of competence, but rather a question of a secure framework. Those who create secure, officially provided access points, establish clear rules for sensitive data, and scale appropriate use cases in a targeted manner can curb shadow AI and unlock its existing potential. The fact that larger companies are already relying on their own AI solutions more often shows that: The need for a secure, in-house platform is clear.



Safe AI Instead of Shadow AI

Without secure access, AI usage quickly shifts to private accounts. This is how shadow AI develops beyond one’s control. Companies need a secure infrastructure that safely enables the productive use of AI.



Security Creates Room for AI

Data protection and compliance must not become obstacles to innovation. A secure framework creates the conditions necessary to use AI productively, without having to halt applications due to uncertainty and leaving valuable potential untapped.



AI Needs Protection at Every Level

Where AI is used particularly extensively, the need to protect sensitive data also increases. That is why, especially at the executive level, clear guidelines and reliable structures are needed to enable the confident use of AI without stifling innovation.

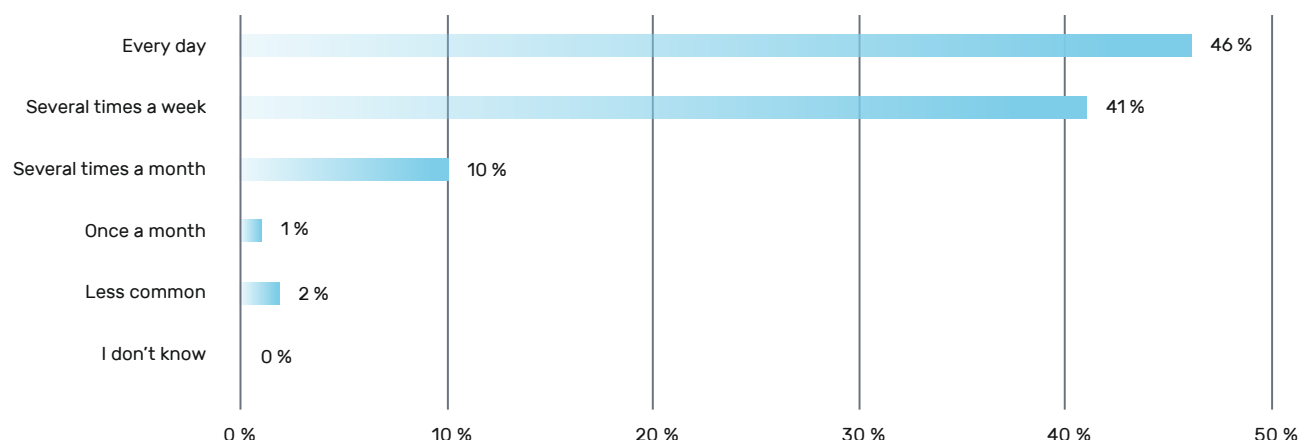


AI is growing. Security scales with growth.

As a company grows, so do its use of AI, the complexity of its AI systems, and the demands placed on them. Having your own secure infrastructure lays the foundation for scaling applications in a controlled manner and permanently integrating AI into existing business processes.

For most people, AI has long been part of their daily work routine

1 How often do you currently use AI applications (e.g., ChatGPT) in your daily work?



Nearly one in two people (46 percent) use AI every day.

AI is used frequently in the workplace: 46 percent already use AI on a daily basis, while another 41 percent use it several times a week. This means that 87 percent use AI at least several times a week. Only a small minority (3%) report using artificial intelligence just a few times a month or even less frequently.

Significant Differences Between Industries

There are clear differences in the frequency of use across industries. In the information technology and telecommunications sectors, AI is used daily by 63 percent of companies; in the finance and insurance sectors, by 59 percent; and in the media and communications sectors, by 55 percent.

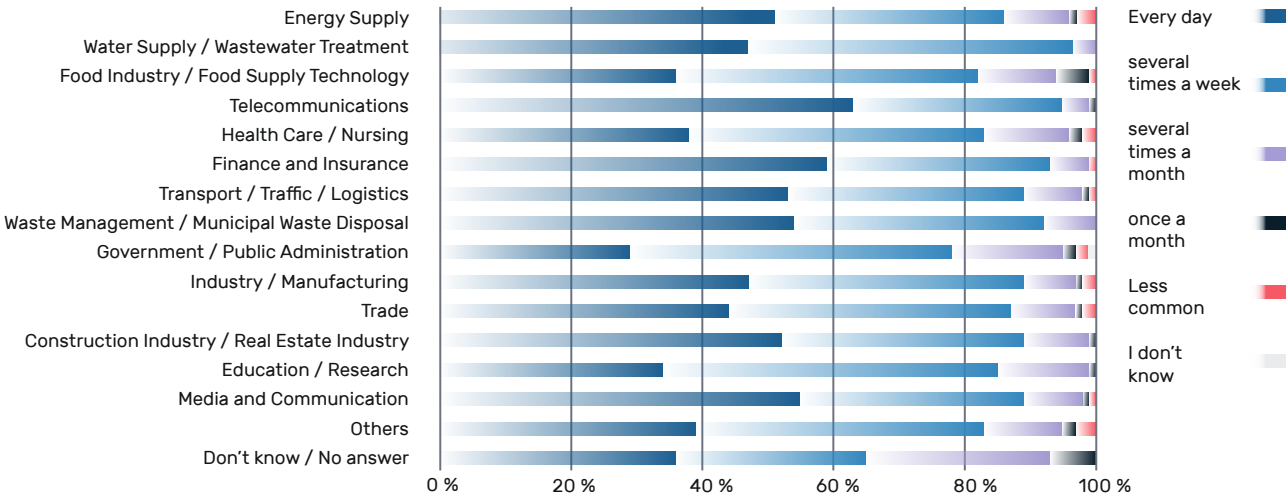
In public administration (29 percent), education and research (34 percent), and the food industry (36 percent), the figures are already significantly lower.

However, AI is also widely used there; the differences mainly concern how often it is used, rather than whether it is used at all: In education and research, 51 percent use AI several times a week, and in public administration, nearly one in two (49 percent) do so as well.

AI is well established across all industries.

The differences are primarily in the intensity of use.

IT, telecommunications, and finance are leading the way.



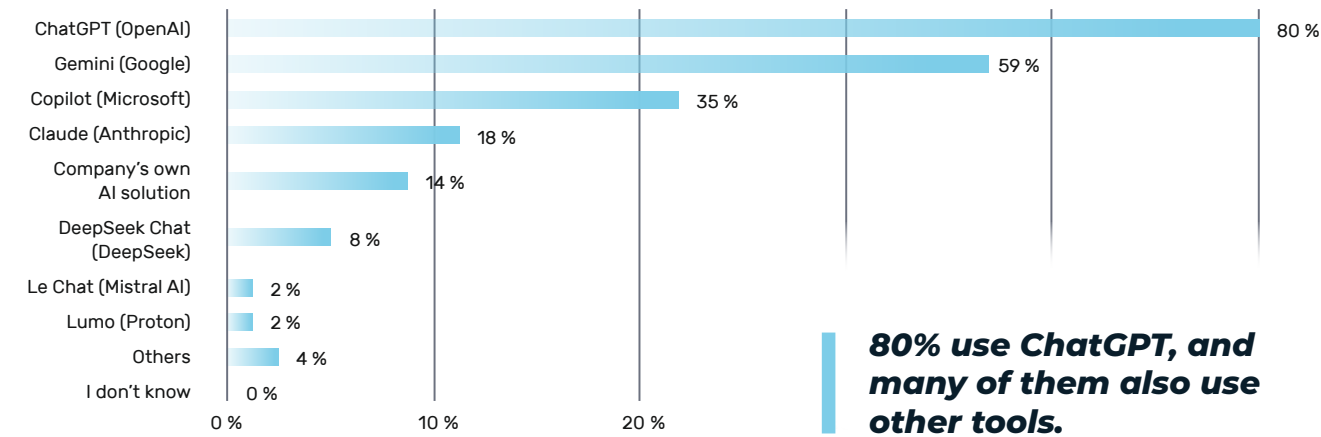
1. USE OF AI APPLICATIONS IN EVERYDAY WORK LIFE

AI has already become an integral part of the daily work routine for professionals who use it. The intensity of use varies particularly significantly depending on the hierarchical level: Managers use AI on a daily basis

significantly more often than employees without managerial responsibilities. Differences by industry, company size, and revenue are also evident, but they are less clear-cut.

OpenAI Dominates the Professional Use of AI

2 What AI applications do you use in your day-to-day work?



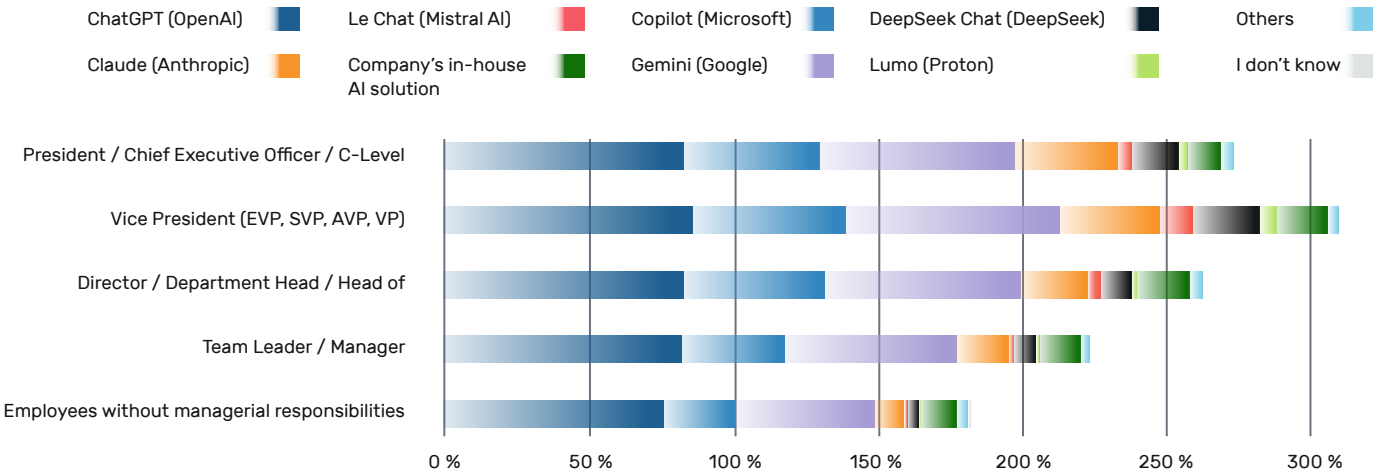
Among working professionals who use AI in their jobs, U.S. tools clearly dominate. ChatGPT (OpenAI) is by far the most widely used tool, at 80 percent. Next are Gemini (Google) with 59 percent, Microsoft Copilot with 35 percent, and Claude (Anthropic) with 18 percent. Non-American solutions such as the Chinese DeepSeek (8 percent) and

European AI systems such as the French Le Chat (Mistral) and the Swiss Lumo (Proton) lag far behind, each at 2 percent. Because multiple responses were allowed, the results also show that many employees use several AI tools at the same time.

Managers use a wider range of tools

The differences by hierarchical level are particularly striking. While ChatGPT remains the leader across all groups, senior management levels are using other AI applications significantly more often. Among vice presidents, for example, 86 percent use ChatGPT, 74 percent use Gemini, 53 percent use Copilot, and 35 percent use

Claude. For employees without management responsibilities, the corresponding figures are 76, 49, 24, and 10 percent. In other words, executives are not only using AI more frequently, but they are also combining different tools to a greater extent. The larger the company, the more institutionalized the toolset.



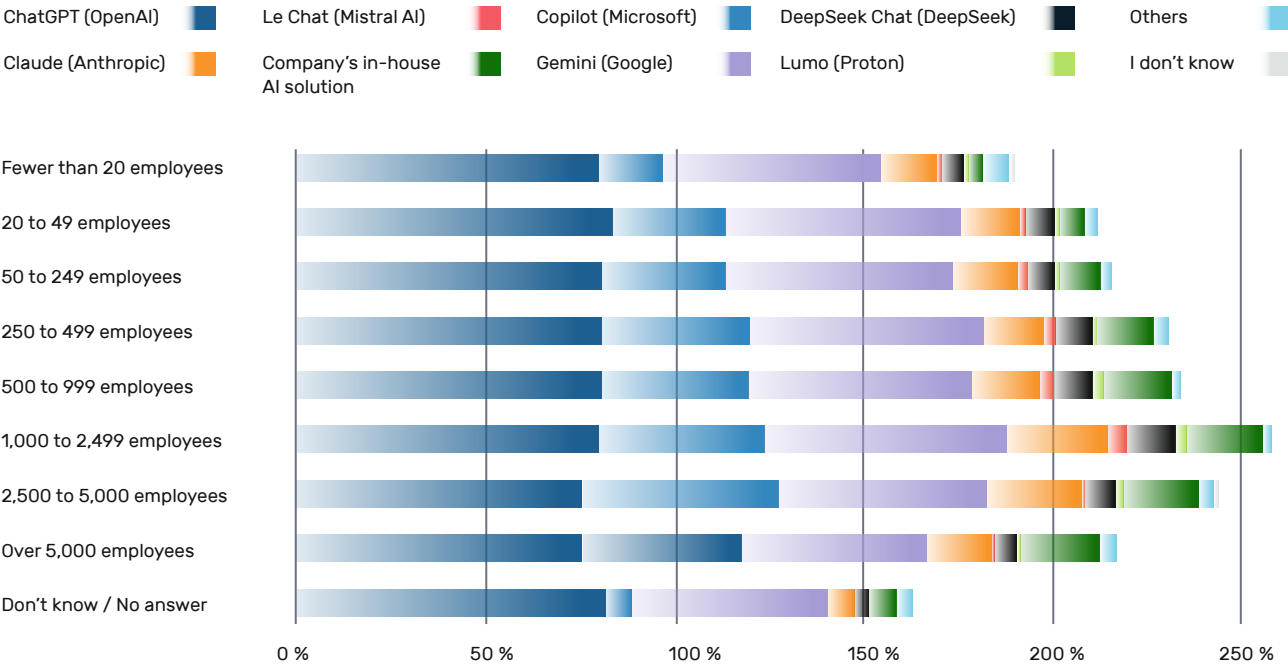
Larger companies are more likely to rely on Copilot and their own AI solutions

As a company grows, it is not so much the use of ChatGPT that changes, but rather the composition of the toolset. ChatGPT remains at a high level of approximately 76 to 84 percent across nearly all size categories.

By contrast, Microsoft Copilot is seeing a much sharper increase: from 17 percent in companies with fewer than 20 employees to 52 percent in companies with 2,500 to 5,000 employees. The pattern is even clearer when it comes to in-house AI solutions. In micro-enterprises (fewer than 20 employees), only 4 percent use them, whereas in companies with more than 5,000 employees, 21 percent do.

Larger companies are therefore relying more heavily on AI solutions provided by their own organizations, while smaller companies are turning to generally available tools.

The use of in-house AI solutions increases by 17% as companies grow in size.



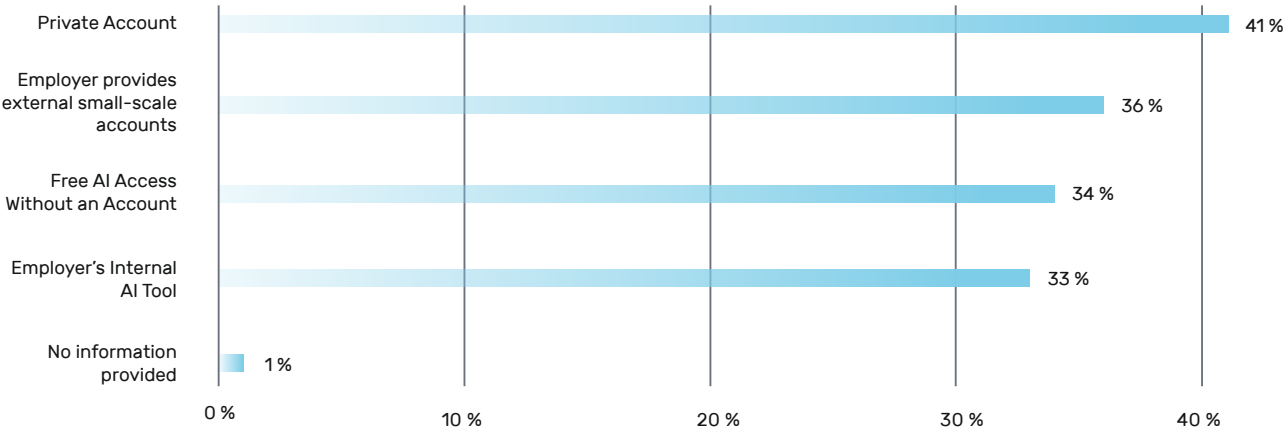
2. THE LARGER THE COMPANY, THE MORE COMMONPLACE AND COMPLEX ITS USE BECOMES. THE NEED FOR A PROPRIETARY, SECURE AI PLATFORM IS CLEAR, AND THE MARKET FOR IT EXISTS.

ChatGPT is clearly the go-to AI tool for everyday work. At the same time, a multi-tool environment is becoming increasingly established. Managers in particular, as well as employees at larger companies with higher revenue, are more likely to use other solutions such as Gemini, Copilot, or in-house AI systems in addition to ChatGPT.

The larger and more organizationally complex a company is, the more the use of AI seems to be shifting from individual, freely available tools toward a broader, more institutionalized set of tools.

Private and provided access points are located close to one another

3 In what ways do you use AI applications for work-related tasks?



Private and employer-sponsored plans are very similar

The professional use of AI takes place through a wide variety of channels. Personal accounts are used most frequently (41 percent). These are followed by external AI accounts provided by the employer (36 percent), free AI access without an account (34 percent), and the employer's internal AI tools (33 percent). Although the data show that many employees apparently use multiple access channels simultaneously, the high proportion of private and freely available access points suggests a significant amount of shadow AI. Much of the professional use of AI thus takes place outside of officially provided and regulated structures.

Shadow AI in the Workplace:
41 percent use personal accounts for work-related tasks.

AI IS FIRMLY EMBEDDED IN EVERYDAY WORK LIFE, OFTEN THROUGH PERSONAL ACCOUNTS. IF A PROVIDED ACCESS POINT IS MISSING, SHADOW AI ARISES. SECURE, COMPANY-OWNED ACCESS IS BECOMING A KEY REQUIREMENT.

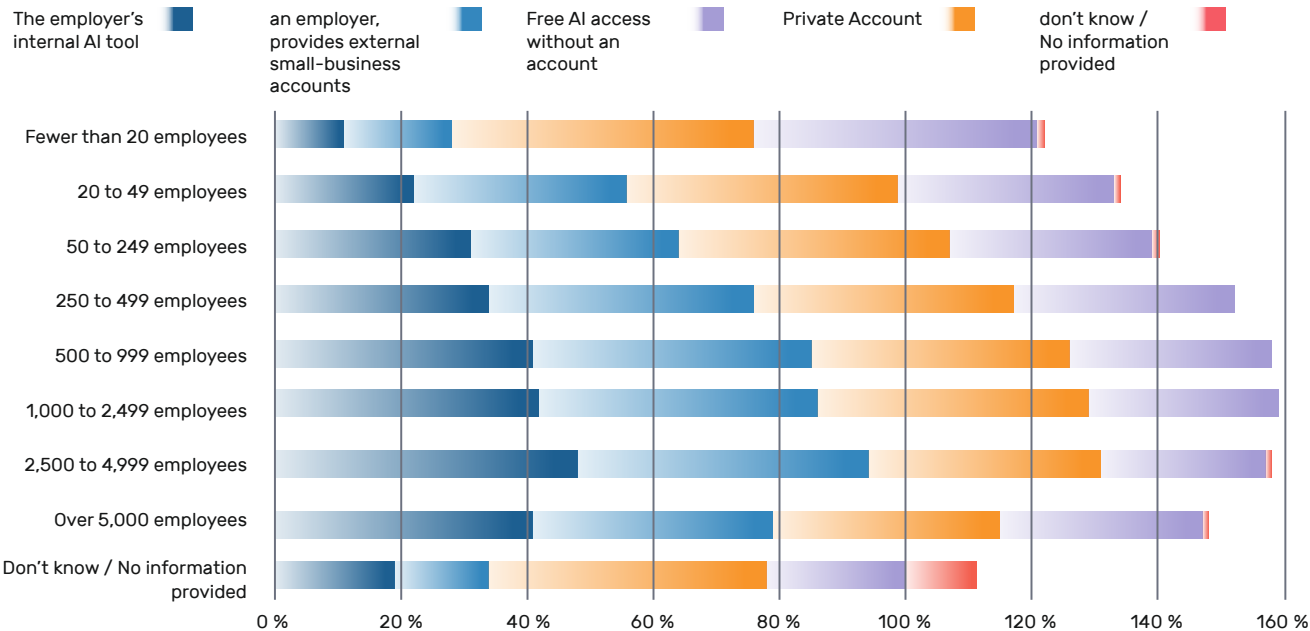
THE HIGHER THE POSITION, THE MORE CARELESS THE HANDLING OF SENSITIVE DATA. THE MOST INTENSIVE USE OF AI AND THE MOST SENSITIVE DATA CONVERGE WHERE THE NEED FOR PROTECTION IS GREATEST.

Managers have more frequent access to provided solutions

The differences are particularly evident across hierarchical levels: Among vice presidents, 53 percent use internal AI tools and 56 percent use external accounts provided by their employer; among employees without management responsibilities, however, these figures are only 24 percent and 22 percent, respectively. Managers, therefore, have more frequent access to officially provided solutions and make greater use of them. Nevertheless, private

accounts play an important role at all levels: Even at the C-level, 52 percent use a personal account; among vice presidents, the figure is 58 percent; and among employees without management responsibilities, it is 43 percent. Even though internal tools are often used at higher levels of the hierarchy, private accounts are still used very frequently alongside them.

The larger the company, the more institutionalized the access



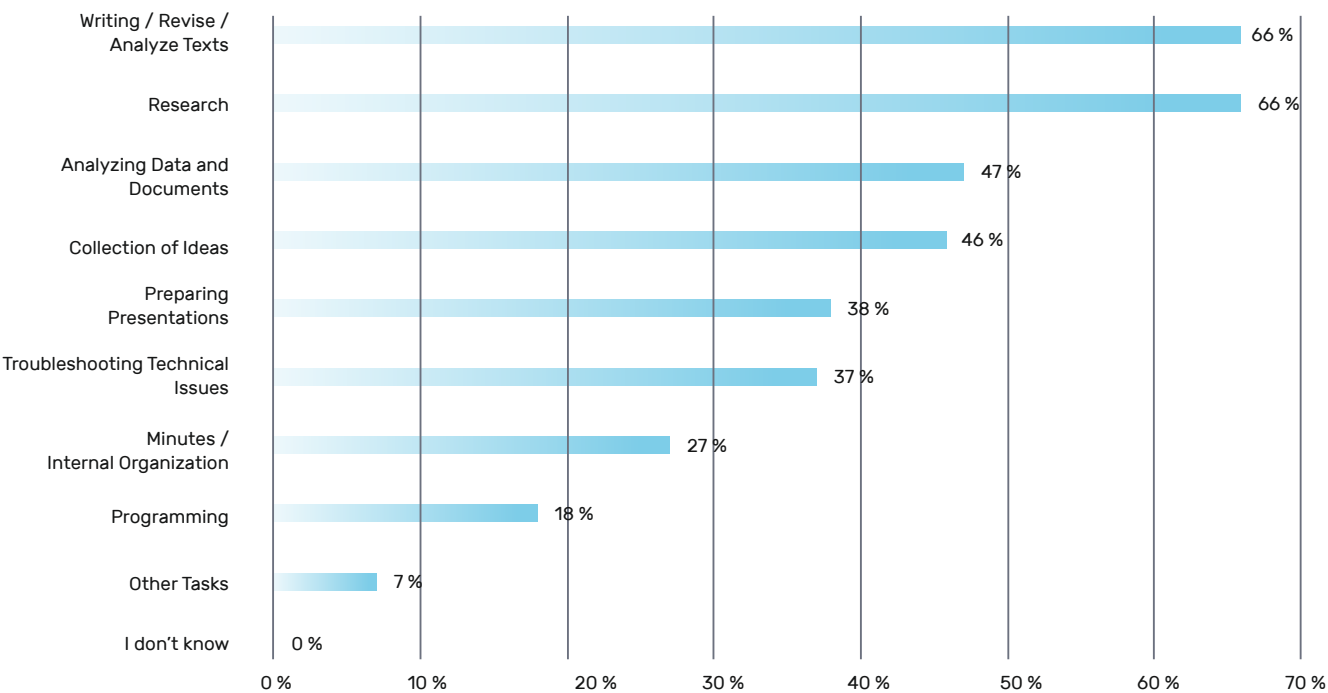
3. AI SYSTEMS NEED OVERSIGHT

Currently, AI is used for work primarily through personal accounts, freely accessible services, or company-provided access to external providers. Only 33 percent of respondents use an internal AI tool provided by their employer. This means that the vast majority of employment data is processed through channels that

are not directly under the company's control. As a company grows, the choice of AI approaches changes: While employees at smaller companies rely more heavily on private and freely available AI offerings, larger companies with higher revenue rely significantly more often on internal tools and officially provided accounts.

AI is, above all, a tool for knowledge work

4 For what tasks do you use AI applications in your day-to-day work?



Writing and research are the most important areas of application

In everyday professional life, AI is used primarily for writing and research. Sixty-six percent use AI to write, edit, or analyze texts, and another 66 percent use it for research. This is followed by the analysis of data and documents at 47 percent and brainstorming at 46 percent. 38 percent use AI to prepare presentations, while 37 percent use it to solve technical problems. Significantly less common are protocols and internal organization (27 percent) and programming (18 percent).

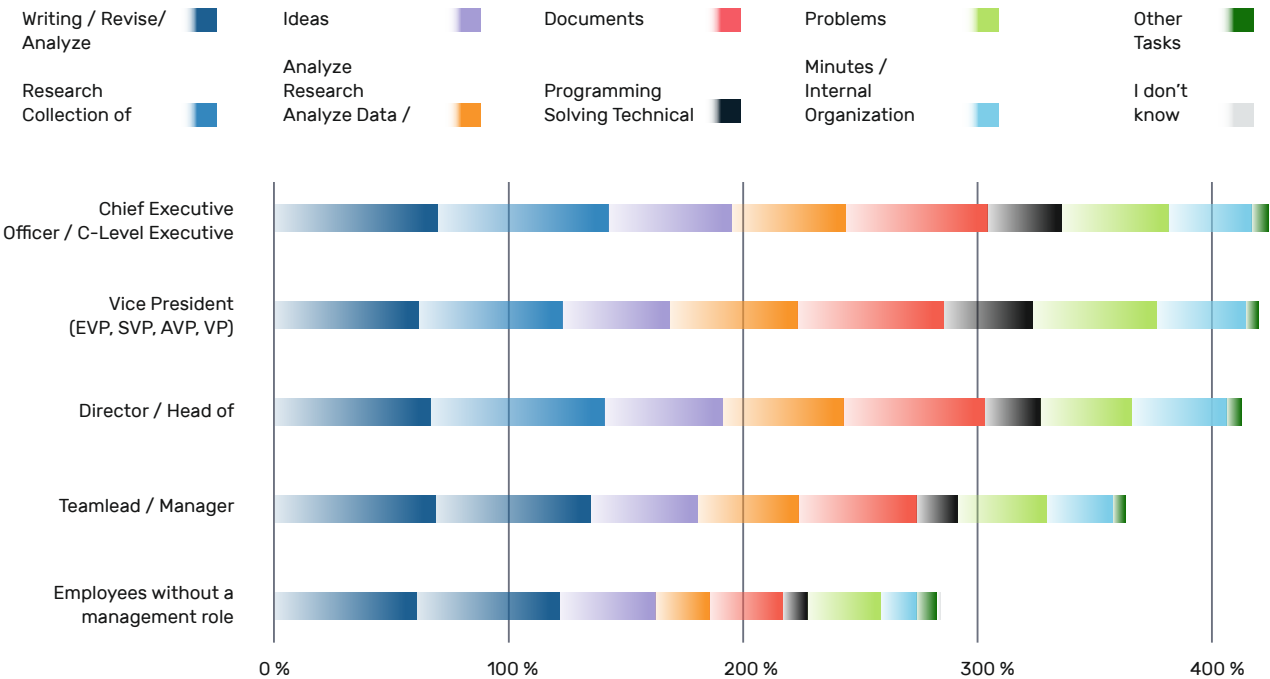
66% use AI for writing and research; the most common applications of AI are writing and research, followed by data and document analysis.

Executives are using AI for a wider range of tasks

As one moves up the organizational hierarchy, the use of AI shifts toward more complex tasks that are more closely tied to work processes. 61 percent of C-level executives and 63 percent of vice presidents use AI to analyze data and documents, compared with just 31 percent of employees without management responsibilities.

The gap is even more pronounced when it comes to preparing presentations: 54 percent of vice presidents, 51 percent of directors and department heads, and 48 percent of C-level executives use AI for this purpose. For employees without management

responsibilities, this figure is only 23 percent. Managers also score higher in areas such as meeting minutes, technical issues, and programming. Without managerial responsibilities, however, the focus is more on writing and research.



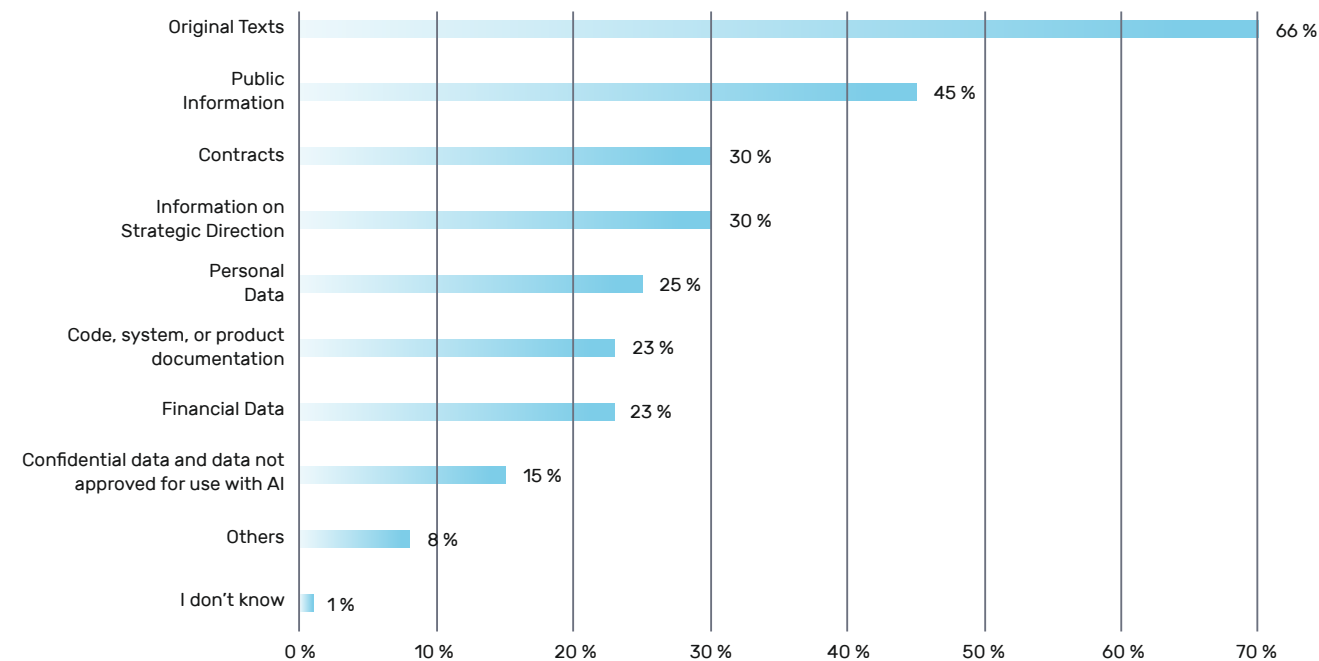
4. FROM ASSISTANCE TO INTEGRATION

In the workplace, AI has so far been used primarily as a tool for knowledge- and communication-related tasks—particularly for writing, research, data analysis, and brainstorming. At the same time, it becomes clear that: Executives and employees at larger companies with higher revenue use AI more frequently for a wider range

of tasks, including data analysis, presentations, and internal processes. As a result, its use there goes beyond individual support tasks and has a more profound impact on existing workflows.

Sensitive data has long been part of AI applications

5 What types of data or information have you already processed using AI applications?



AI isn't just used for non-critical content

AI has long been used in everyday work, even when dealing with sensitive content. Thirty percent have already used AI to process contracts or strategic information, 25 percent have used it to process personal data, and 23 percent have used it to process financial data. Particularly relevant: 15 percent specifically mention data that is confidential or not authorized for use by AI. Thus, its use clearly extends beyond non-critical tasks and touches on areas where data protection and confidentiality are subject to particularly stringent requirements.

15% have used AI to process data that is explicitly confidential or not authorized for use with AI.

At higher management levels, the figures are significantly higher

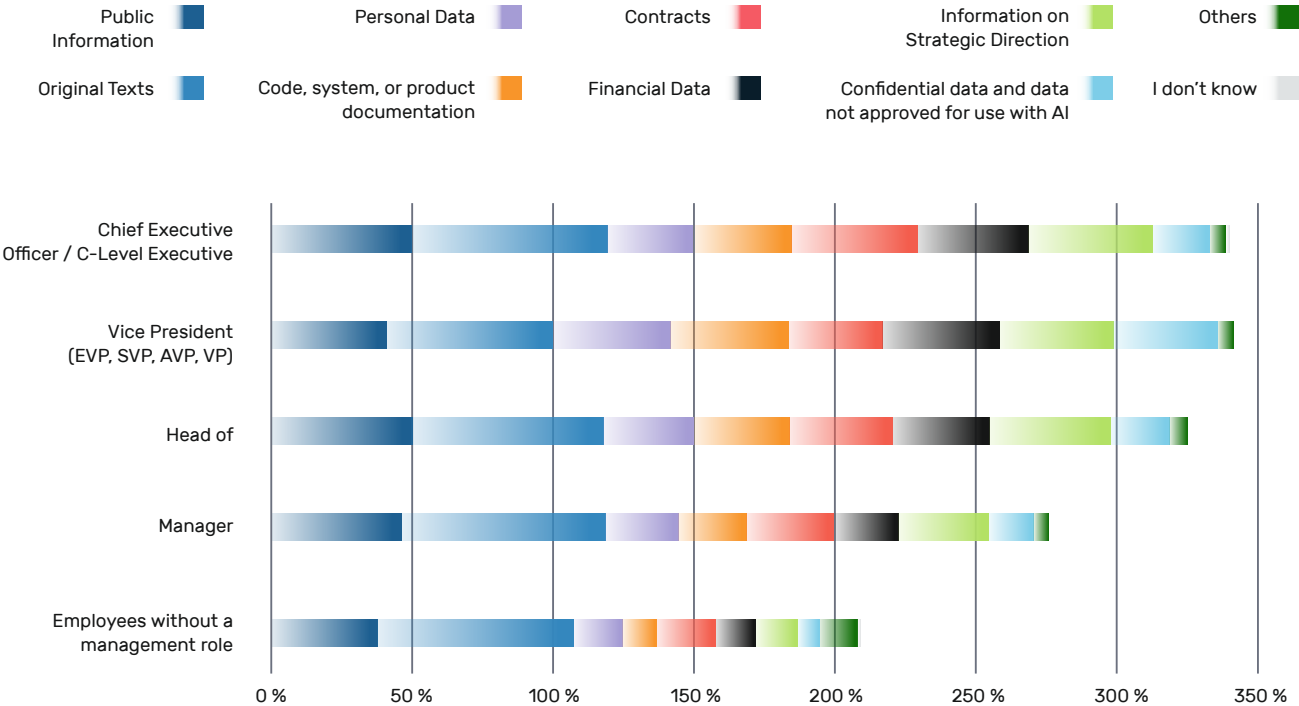
The amount of sensitive data one handles increases with one’s position in the company. At higher levels of management, the proportion of personal data, contracts, strategic information, and financial data processed using AI is often significantly above average.

It is precisely those employees who work with AI most frequently and extensively who are also most likely to handle information requiring special protection.

Consequently, the risk increases precisely where the need for protection is greatest.

AI REQUIRES CONTROLLED ACCESS

Data requiring special protection is increasingly being processed using AI in everyday professional life. To this end, companies must provide secure, controlled AI solutions—otherwise, they risk having confidential information fall into hands beyond their control through private or publicly available access points.

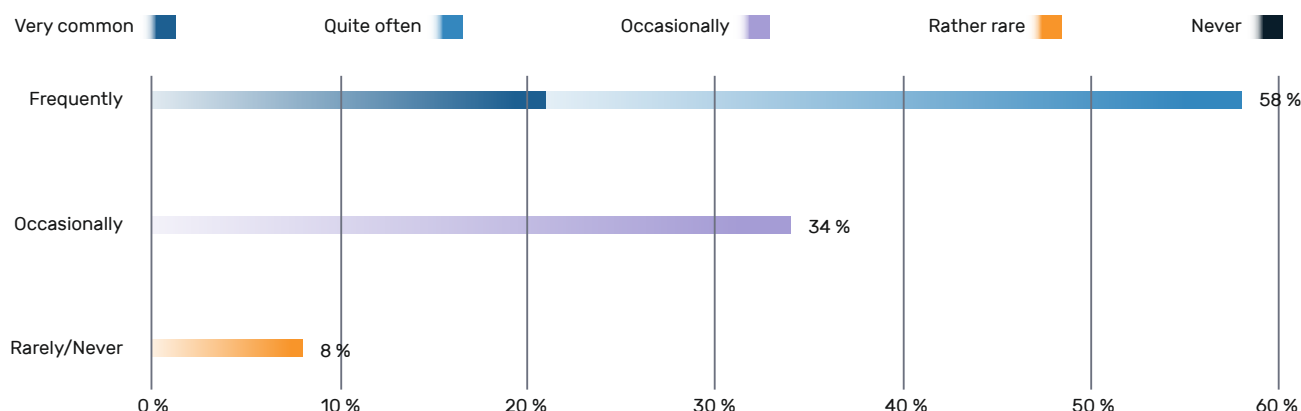


5. SENSITIVE DATA REQUIRES SECURE AI

Although AI is primarily used for creating original texts and public information, that is by no means its only use. A significant portion of professionals who use AI also process personal data, contracts, financial data, strategic information, or even confidential or restricted content. This is particularly pronounced at higher levels of management. This makes it clear that issues related to data protection, information security, and governance are an integral part of the day-to-day use of AI in companies.

A great deal of potential remains untapped in day-to-day work

6 How often do you complete tasks without using AI, even though AI could have helped you with them?



The potential of AI often goes untapped in everyday work

Even though 87 percent of respondents use AI at least several times a week, they still complete many tasks without AI support. 58 percent say that this happens frequently. For another 34 percent, this is at least occasionally the case. Only 8 percent say this is rarely or never the case. This means that 92 percent fail to take advantage of the potential assistance offered by AI, at least occasionally. So even among experienced users, the available potential is far from being fully realized.

In many cases, 92% do not fully leverage the potential of AI.

SECURITY UNLOCKS THE POTENTIAL OF AI

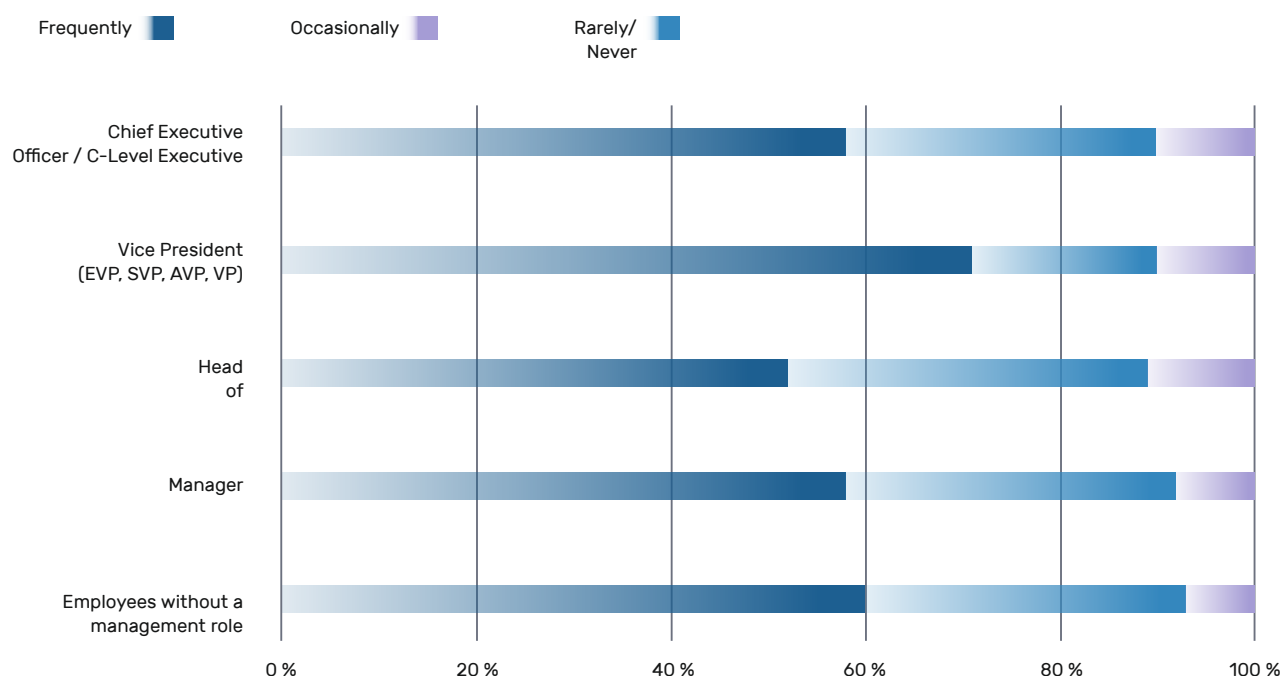
Much of AI's potential remains untapped. A structural pattern that extends across all sizes and levels, not isolated cases. A secure framework maximizes potential.

The gap between available and actually utilized AI support is evident regardless of organizational level, company size, revenue, or industry. No clear pattern is apparent: Among executives, the percentage of those who frequently fail to take advantage of potential AI support ranges from 52 percent among directors and department heads to 71 percent among vice presidents.

Company size and revenue also do little to explain the differences. Depending on the size of the company,

the figures fall within a narrow range between 55 and 63 percent. In terms of revenue, the figures range from 51 to 62 percent; even among companies with at least five billion euros in revenue, 59 percent report that they often do not make use of available AI support.

The same pattern is evident across all industries: The figures range from 53 percent in the manufacturing sector to 77 percent in the waste management sector. Unutilized AI potential is therefore not a marginal phenomenon in any of the groups examined.



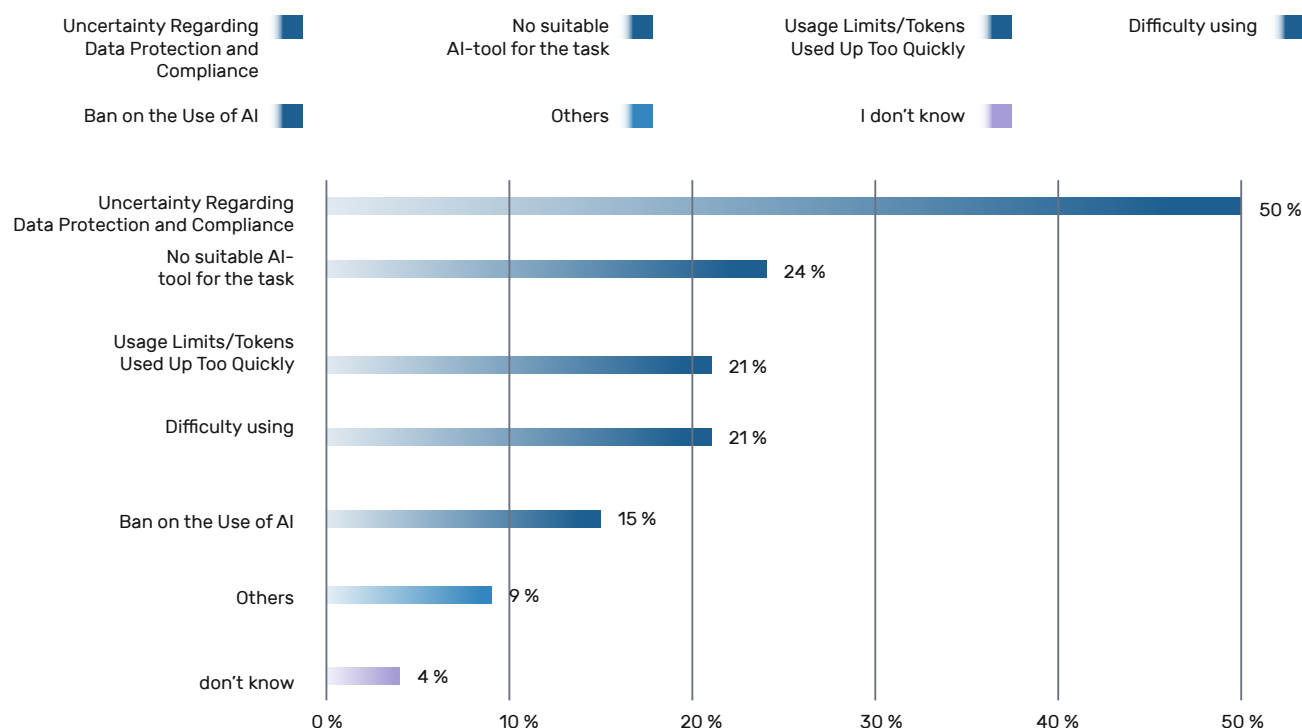
6. CONSISTENTLY INTEGRATE AI INTO PROCESSES

Untapped AI potential is not an isolated case; rather, it is evident across all organizational levels, company sizes, revenue brackets, and industries. Employees regularly perform tasks without AI support, even though such support is generally possible and would often be helpful.

The bottleneck, therefore, lies not solely in the availability of AI, but in integrating it securely, effectively, and seamlessly into work processes.

Data protection and compliance are the main bottleneck

7 For what reasons have you already decided not to use AI or stopped using it?



Data protection and compliance are the biggest obstacles

The most commonly cited reason for not using AI is uncertainty regarding data protection and compliance. As a result, 50 percent have already decided not to use an AI application or have stopped using one. Other barriers, such as a lack of suitable tools, usage limits, or difficulties in using the software, lag far behind. The biggest bottleneck, therefore, often lies less in the technology than in the organizational framework. This is evident across almost all company sizes.

In companies with fewer than 20 employees, 41 percent cite data protection and compliance concerns as the reason; in companies with more than 5,000 employees, the figure is 54 percent. For companies with revenue of at least 100 million euros, that share rises to 59 percent. A more institutionalized AI infrastructure therefore does not automatically resolve governance issues.

One in two people has already opted not to use AI due to data protection and compliance concerns.

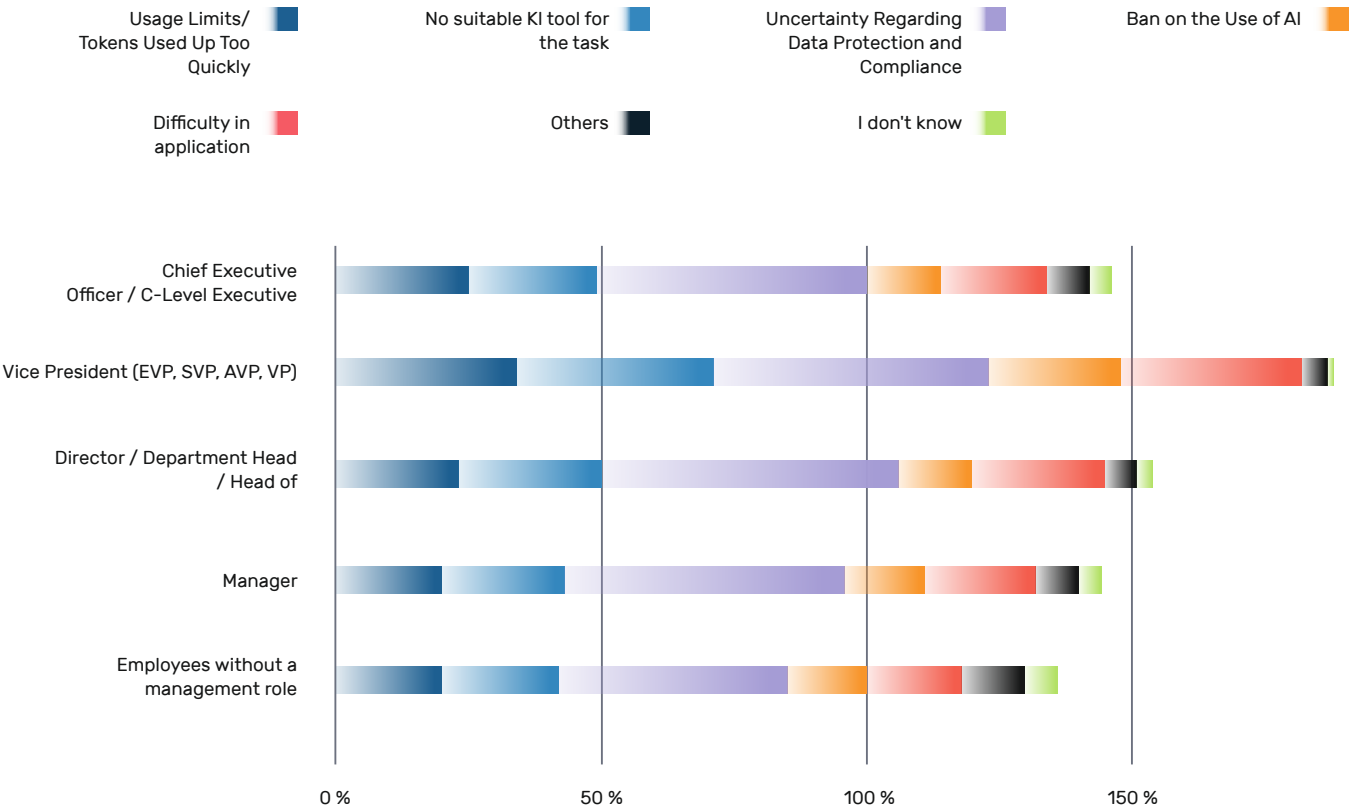
SAFETY LEADS TO PRODUCTIVITY

Data protection and compliance are the key bottleneck. The bottleneck is not a matter of competence, but rather a question of a secure framework. Where it is lacking, productivity suffers.

Executives are more likely to run into technical limitations

As one moves up the organizational hierarchy, however, the number of technical hurdles in the professional use of AI does increase. Among vice presidents, 37 percent cite a lack of suitable AI tools, 34 percent cite usage limits, and another 34 percent cite difficulties in using them. For employees without managerial responsibilities, the

corresponding figures—22, 20, and 18 percent—are significantly lower. An indicator that executives are using AI more frequently for more complex, extensive, or strategically important tasks—and are thus reaching the limits of available tools more quickly.



7. UNCERTAINTY IS SLOWING DOWN THE ADOPTION OF AI

The main obstacle to the professional use of AI is uncertainty regarding data protection and compliance: as a result, 50 percent have already opted not to use AI or have stopped using it.

Other barriers play a significantly smaller role. Thus, it is not so much the availability of AI that determines its productive use, but rather whether it can be used safely and in compliance with regulations.

Creating Secure AI Access, and Curbing Shadow AI

1

Companies must provide secure, officially approved, and easy-to-use AI access for all relevant employee groups.

Only 33 percent of professional AI users currently use an internal AI tool provided by their employer, while 41 percent use personal accounts and 34 percent use freely accessible services that do not require an account. The majority of professional AI use therefore often still takes place outside of directly controlled corporate systems.

Powerful, secure alternatives can reduce “shadow AI” and bring professional data back into manageable structures.

2

Establish Clear Rules for Sensitive Data

Companies should establish binding guidelines specifying which data may be processed in which AI environments and which types of content are excluded.

50 percent have either not used an AI application or have stopped using it due to concerns about data protection and compliance—significantly more often than due to a lack of suitable tools, usage limits, or difficulties in using the application. Clear guidelines, data classification, and a clearly communicated list of approved AI tools provide guidance and lower this barrier.

Scale AI Deployment in a Targeted Manner

3

Companies should integrate the selective use of AI into specific, secure standard processes. Although 46 percent use AI daily and another 41 percent use it several times a week, 92 percent still complete tasks without AI at least occasionally, even though it could provide support.

Companies should therefore prioritize use cases that offer high value and have a clear risk profile, rather than leaving the use of AI solely up to individual employees. For executives and other heavy users, there is also a need for high-performance solutions tailored to their specific tasks: Vice presidents report a lack of suitable tools, usage limits, and difficulties in using them significantly more often than employees without managerial responsibilities.

AI ADOPTION REPORT
Myra Security, 2026

Scan the QR code to access the digital version of the study, as well as supplementary materials and additional information.



Methodological Note: The results are based on a Civey survey of 4,000 working adults who use AI in their professional lives in Germany. It was conducted from August 5 to August 14, 2026. The survey was conducted online. For questions allowing multiple answers, respondents could select more than one category. The statistical margin of error is approximately ± 2.5 percent. Data was provided by Civey. As of August 26, 2026.

Note on Language and Gender Inclusion: For the sake of readability, the generic masculine form is used in this report. Unless otherwise explicitly stated, all references to people apply equally to all genders.

Made in Germany



Myra protects what matters most. In the digital world.

Would you like to learn more about how our solutions can help you increase your revenue, minimize your costs, and protect your applications from malicious attacks? Our team of experts will be happy to provide you with personalized advice and develop a customized solution for your organization. We recommend that you schedule a no-obligation consultation today.

Cyberattacks are expensive, but a no-obligation consultation costs nothing.

Myra Security GmbH

☎ +49 89 414141 - 345
🌐 www.myrasecurity.com
@ info@myrasecurity.com