PESTALOZZI

ATTORNEYS AT LAW

Navigating AI with Pestalozzi

A Practical Legal Guide

PESTALOZZI'S PRACTICAL LEGAL GUIDE FOR AI

Since its launch in November 2022, ChatGPT has taken the world by storm, marking a significant milestone in technological advancement. The pace of innovation in AI partnered with its easy access both to the broader public and specialized users shows no signs of slowing down. Along with a sizable increase of new offerings and startups entering the market, its future remains highly promising. As companies increasingly embrace AI for creating content and optimizing their processes, the attraction of its benefits is accompanied by the necessity to mitigate the risks associated with the technology.

In this ever-changing landscape, finding the middle ground between leveraging AI's capabilities and safeguarding against its risks is paramount. Navigating AI with Pestalozzi: A Practical Legal Guide serves as a practical manual for Swiss companies to identify key legal issues and navigating the complexities of introducing and using AI internally. Through our six-part series, curated in this Guide, we provide a pragmatic overview of critical issues focusing on corporate governance, regulation, liability, data protection, intellectual property, and employment.

AI changes the world as we know it. We explore its potential together with our clients and provide legal advice.

TABLE OF CONTENTS

PART 1: AI GOVERNANCE

Key Takeaways

A clear allocation of the different levels of responsibility regarding AI is essential for a safe use of AI tools.

Establishing policies and (ethical) guidelines, regular audits, and trainings to raise awareness are key to mitigating risks posed by AI.

AI governance is not a linear process, which can be completed once, but is cyclical in nature and must be continually evaluated and revised.

NECESSITY OF AI GOVERNANCE

AI presents substantial savings and opportunities for companies, which drives its adoption across nearly all sectors. Nevertheless, according to the December 2023 IAPP-EY Professionalizing Organizational AI Governance Report, 57% of European companies indicated that they do not control their use of AI. Integrating AI into products and internal processes without robust AI governance entails significant legal, financial, and reputational risks. While Swiss law currently does not provide specific regulations for AI, it does emphasize the board's responsibility to oversee AI initiatives as part of their general duties. In addition, the extraterritorial scope of regulations like the EU AI Act, which establishes comprehensive compliance obligations for providers and users of AI applications, makes it insufficient to consider only national laws. Regardless of whether the EU AI Act applies to your company, AI governance should be a top priority for the board of directors of Swiss companies. Ideally, this governance should be considered before the implementation of AI projects.

Effective AI governance balances the need for innovation with the imperatives of compliance with existing regulations, ethical considerations, and commercial value. The framework should be as adaptive as AI itself, focusing on a risk-based approach that evaluates the likelihood of harm occurring, the severity of that harm, and appropriate mitigation measures associated with each AI use case. This chapter offers practical guidance on establishing a robust and dynamic AI governance framework in a company. It focuses on key elements, such as allocating responsibility and possible implementation methods of AI governance. Ultimately, each company should tailor its AI governance program to meet its individual business needs and objectives.

Effective AI governance balances innovation with compliance, ethical considerations, and commercial value.

ALLOCATING RESPONSIBILITY

A successful AI governance framework is built on clearly defined roles, responsibilities and decision-making processes. Assigning accountability is essential to ensuring that AI initiatives align with organizational goals and defined ethical standards.

1. **Board:** The board of directors is responsible for overseeing all major company initiatives, including AI. This oversight includes understanding the potential risks associated with AI and ensuring that proper governance frameworks are in place to mitigate these risks, and that adequate staffing is ensured. Also, the board's involvement is crucial for aligning AI strategies with the company's goals and values, and for setting an effective tone from the top. The board of directors might also invite experts or external advisors to provide

feedback on the company's AI governance strategy. Furthermore, it should be determined how the board will be regularly and appropriately informed about AI developments by the management or other functions, such as the AI committee (see below).

2. **Management:** While the board has ultimate oversight, the day-to-day management and operationalization of AI strategies are typically delegated to the management. Management is responsible for developing AI policies, integrating AI into business processes, and ensuring compliance with governance frameworks set by the board. The actual monitoring of adherence to regulations and internal policies should be delegated down to project leaders (see below), compliance or HR department.

   Management must also assess the impact of AI on various aspects of the business, such as efficiency, risk, and competitiveness, and regularly report these findings to the board. It also plays a key role in the coordination and collaboration across various functions within the organization. This includes working closely with the AI committee to ensure that AI initiatives are aligned with governance frameworks, and that all relevant departments, such as IT, legal, compliance, and business units, contribute effectively to AI projects. Furthermore, management must ensure that project leaders are appointed for each AI initiative. By embedding AI governance responsibilities within the management structure, the company can achieve a cohesive and effective implementation of AI that supports its strategic objectives.

3. **AI Committee:** Management should consider establishing an expert AI committee / task force with employees from different backgrounds, such as IT, finance, legal, compliance, risk management, and from different business units. Evaluating governance issues related to AI increasingly requires a deep understanding of the technology context. These challenges require breaking down silos and working closely together on an ongoing basis, especially between legal, compliance and IT teams.

   The committee should meet regularly and be the driving force within the company to promote and ensure a value-adding implementation of AI by:

   - Mapping and monitoring how AI systems are being used internally,
   - drafting of internal guidelines and processes for the deployment of AI and development of use cases, including best practices,
   - keeping the board and management informed about technological and regulatory developments; and
   - training employees on appropriate and effective use of AI.

4. **AI Project Leader:** For each AI initiative, a project leader should be designated to manage the day-to-day operations, ensure adherence to governance policies, and report progress to the AI committee and/or management. No AI use case should proceed without an assigned project leader responsible for following internal policies.

Reporting Structures

Establishing clear reporting structures will ensure that AI governance is effectively implemented and maintained. The AI committee should be in regular contact both with the AI project leaders as well as legal, compliance and IT teams to provide guidance and support. In turn, the AI committee should report regularly to the management and assist management in its reporting to the board on AI governance matters. A company with intensive use of AI is advised to make this report on a quarterly or semi-annual basis. In addition, a company-wide reporting system will help both the AI committee and the AI project leaders to be informed about the performance or reported problems of AI systems. Finally, clear escalation pathways should be defined.

Embedding Responsibilities in Bylaws

Defining AI governance responsibilities in corporate bylaws and policies both increases accountability and limits liability. The more specific the bylaws and policies, the better the company and its directors are protected from potential liability under Swiss law. Therefore, in particular the relevant policies should clearly state the structure of the company's AI governance system, the division of responsibilities, and the allocation of duties with respect to AI governance. Expanding the bylaws to include AI governance is the board's responsibility.

Defining AI governance responsibilities in corporate bylaws and policies both increases accountability and limits liability.

RISK ASSESSMENT

Effective AI governance requires robust risk management practices to identify, assess, and mitigate potential risks associated with AI deployment.

First, a risk assessment framework specific to AI projects should be developed. This should include identifying potential risks, such as data breaches, ethical violations, and operational failures, and assessing their impact and likelihood. Second, strategies to mitigate identified risks should be defined, documented, and implemented. This could involve technical measures, such as encryption and anonymization of (personal) data, as well as organizational measures, such as internal guidelines (see below), employee training and awareness programs. Finally, an incident response plan to address AI-related incidents promptly should be established. This plan should outline the steps to be taken in the event of a data breach, ethical violation, or other AI-related incidents.

Risk assessment and management are of particular relevance in the following areas: Data protection and cybersecurity (see Part 4: Data Protection), intellectual property rights (see Part 5: Intellectual Property), and employment related issues (see Part 6: Employment).

INTERNAL POLICIES AND GUIDELINES

Based on the risk assessment, the implementation of internal guidelines that address both legal and (non-legal) ethical principles are crucial for effective AI governance. While legal requirements are defined by the regulators to which the company is subject, ethical standards are to be established by each company individually. Companies need to define acceptable and prohibited AI practices, set guidelines for transparency and quality standards, and develop assessment procedures.

There are various proposals of AI guidelines or principles from international organizations and authorities that can be used as a source of reference. Following the key principles recommended by the EU for achieving trustworthy AI, we recommend:

- **Human Agency and Oversight:** Companies should respect human autonomy and fundamental rights and ensure users can understand and interact with AI. There should always be human oversight, allowing individuals to override AI decisions when necessary.
- **Technical Robustness and Safety:** AI systems must be secure, reliable, and robust enough to handle errors and inconsistencies throughout their lifecycle. This includes cybersecurity measures and processes to assess and mitigate safety risks.
- **Privacy and Data Protection:** Compliance with data protection regulation is mandatory. AI systems that are used should protect privacy and personal data, using techniques like anonymization and data encryption.
- **Transparency and Avoidance of Bias:** Data sets and processes used in AI development should be documented and traceable. AI systems should be identifiable as such, and their decisions must be explainable and understandable to humans, especially in high-stakes applications like healthcare and finance. AI tools should be regularly audited to ensure they are using appropriate data quality, operating fairly and not perpetuating bias.
- **Accountability:** Mechanisms to ensure responsibility and accountability for AI systems are essential. This includes independent audits, reporting negative impacts, and impact assessment tools. Decisions on ethical trade-offs should be continuously reevaluated.

AI policies should be coordinated with existing data protection, IT, and HR directives.

Once these principles are established, they should be documented and translated into actionable instructions for employees. Smaller companies may use concise general guidelines in a one-pager format, while larger companies with different use cases are advised to create an overarching AI strategy along with more detailed policies and directives for different implementation areas. This ensures that the information is available in a digestible and clear manner, and that employees know where to look for relevant information and understand their responsibilities when using AI.

AI policies should be coordinated with existing data protection, IT, and HR directives. Some documentation obligations in the EU AI Act, for example, overlap with regulations in the GDPR and the Swiss Act on Federal Data Protection. One such obligation is the data protection impact assessment, which should be conducted when new technologies are implemented (see Part 4: Data Protection).

Furthermore, it is generally advisable to involve legal counsel familiar with regulatory requirements, when drafting internal guidelines and implementing the governance framework to ensure adherence to legal standards. This includes compliance with data protection laws, industry-specific regulations, and emerging AI-specific legislation (see Part 2: Regulation).

10 PRACTICAL STEPS TO IMPLEMENT AI GOVERNANCE

Phase 1

Assess Current Governance Structures Regarding AI

During a first preparatory phase, a company should assess its current "point of departure" to identify gaps in governance respectively areas to be focused on by means of:

1. Internal Audit: Evaluate existing or potential AI use cases, existing governance structures, data management practices, and the regulatory landscape in which the company operates. Instead of implementing new AI-specific governance processes, it makes sense to integrate AI governance measures into existing processes wherever possible.
2. Stakeholder Analysis: Identify key stakeholders and their roles in AI governance. Assess their expectations and readiness to participate in AI governance initiatives.

Phase 2

Develop an AI Governance Framework

During the second phase, a company should develop a comprehensive AI governance framework tailored to its specific needs. This includes:

3. Allocation of Responsibility: Establish four levels of responsibility, led by board oversight, operational responsibility with management with the support of a dedicated AI committee, and executed by an AI project leader.
4. Risk Assessment: Identify potential risks associated with AI deployment by developing a risk assessment framework, and define and implement strategies to mitigate risks as well as a response plan to incidents.
5. Policy Development: Based on the risk assessment, establish internal guidelines addressing legal and ethical principles for effective AI governance, defining acceptable practices, transparency, and quality standards. Coordinate AI policies with existing internal governance frameworks, and involve legal counsel to ensure compliance with regulations and emerging AI-specific legislation.
6. Pilot Projects: It may be advisable to implement pilot projects to test the governance framework first to identify potential issues and to refine the governance framework before rolling it out company-wide.

Phase 3

Implement the Framework

The last phase focuses on the roll out the AI governance framework across the organization. Successful implementation and monitoring of an AI governance framework includes:

7. Training and Communication: Ensure that the newly implemented AI policies get the necessary attention internally. Conduct training and education sessions for employees at all levels to familiarize them with the use of AI in accordance with the company's internal policies. Point out key topics such as AI ethics, data management and compliance and emphasize the importance of not uploading confidential information to an AI system as well as that output should always be subject to human review before use.
8. Regular Reviews: Led by the AI committee, AI governance frameworks should be reviewed periodically to adapt to new regulations, technological advancements, emerging risks and experienced failures. Review also the performance of AI systems to ensure they operate as intended and are in line with the implemented AI governance framework and regulatory requirements.
9. Feedback Loops: Establish feedback loops to gather input from stakeholders, including employees, management and customers. Use this feedback to make necessary adjustments.
10. Industry Collaboration: Engage with industry bodies and participate in forums to stay updated on best practices and emerging trends in AI governance.

PART 2: REGULATION

Key Takeaways

Determine the applicable law, in particular by reviewing specific contracts or the AI provider's terms and conditions for an applicable law clause. In addition, assess where your AI providers and customers are located, and the geographic reach of the personal data streams and IP rights involved.

If Swiss law is applicable: Switzerland does not have an overarching regulation concerning AI. Instead, AI applications are governed by the existing legal framework.

Assess whether your company is subject to the extraterritorial reach of the EU AI Act due to an EU connection.

Update yourselves regularly about new regulations and interpretations of existing regulations, as the regulatory landscape is currently changing rapidly.

INTRODUCTION

Companies implementing AI face a complex legal and regulatory terrain that requires careful evaluation. The legal framework surrounding AI is constantly evolving, encompassing both national statutes and international conventions. AI regulations were first introduced in China, underscoring the country's proactive approach to AI governance. This was followed by President Biden's Executive Order on AI on 30 October 2023, prioritizing the safe and trustworthy development of AI in the United States. Furthermore, the wide-ranging Artificial Intelligence Act entered into force on 1 August 2024 ("EU AI Act"), aiming to create a comprehensive regulatory framework for AI in the EU.

MAP OUT THE RELEVANT REGULATORY FRAMEWORKS

Given the global nature of the AI ecosystem, identifying the relevant jurisdictions can be challenging. In order to determine and review the relevant legal framework and consider rights and obligations thereunder, it is essential for every company to first map out the applicable law for each individual use case by analyzing:

- Implicitly or explicitly agreed contractual provisions, including general terms and conditions ("GTC"), of AI providers;
- the seat or domicile of involved AI providers and the company's customers; and
- the geographic reach of the personal data streams and IP rights concerned.

To assess the relevant legal framework and consider associated rights and obligations, companies must first map the applicable laws for each specific use case.

As many jurisdictions to date lack an AI-specific regulatory framework, companies need to rely on contractual protections to guard against potential challenges posed by AI applications. Typically, contracts between AI providers and acquiring companies ("AI-deploying companies") include a choice of law clause that specifies which legal framework governs their agreement. For example, the most prominent AI provider, ChatGPT, designates U.S. law, specifically the laws of the State of California, as applicable in its GTC. Microsoft specifies in its GTC for its Copilot plug-ins that the applicable law depends on the user's location – for companies located in Europe, the applicable law is the law of Ireland. With smaller AI providers, there may be more flexibility in negotiating the choice of

law (e.g., in favour of Swiss law) depending on bargaining power. In view of the principle of party autonomy and the commercial setting, these choice of law clauses are generally upheld by the courts unless they are abused to deprive a party of rights, which are fundamental to the country in which the court is seated.

While intellectual property rights are generally governed by the law of the state for which protection is sought, data protection laws often provide for a certain extraterritorial reach, being applicable to the processing of personal data that has an effect in that state, even if processed abroad.

NO LEGAL VACUUM IN SWITZERLAND

In Switzerland, there is currently no legislation or overarching regulation that specifically addresses AI. This does not imply, however, that AI operates in a legal vacuum. Rather, AI applications are governed by the prevailing general legal and regulatory frameworks.

The Federal Council, Switzerland's executive body, is closely monitoring AI's potential legal and regulatory implications. In contrast to the European Union, which aims at addressing the technology comprehensively as such (horizontal regulation), Switzerland has, so far, promoted an agile, sector-specific regulatory strategy: Measures should be taken, if necessary, in the relevant sectors based on the existing legal framework and in a technologically neutral way.

Unlike the EU's comprehensive, technology-wide approach, Switzerland has so far adopted an agile, sector-specific regulatory strategy.

The emerging international rules and standards, especially the EU AI Act, which entered into force on 1 August 2024, will, however, have a direct impact on Switzerland. The Federal Council therefore mandated the Federal Department of the Environment, Transport, Energy and Communications last year to identify the need for action and possible options for sectoral and, if necessary, horizontal measures by the end of 2024. This report will form the basis for a legislative proposal expected in 2025. Furthermore, on 17 May 2024, the Committee of Ministers of the Council of Europe adopted the Convention on Artificial Intelligence, attended by the head of the Swiss Federal Department of Foreign Affairs. The convention's aim is to ensure compliance with the legal standards applicable to AI in terms of human rights, democracy, and the rule of law. Switzerland was actively involved throughout the negotiations.

If the regulatory assessment of your individual AI use case leads to the conclusion that Swiss law is applicable, the following federal statutes should be carefully considered in the context of AI (non-exhaustive list):

- Swiss Code of Obligations (SR 220), in particular Art. 41 et seqq. and 97 et seqq. with regard to liability and Art. 319 et seqq. with regard to employment aspects;
- Product Liability Act (SR 221.112.944);
- Data Protection Act (SR 235.1);
- Copyright Act (SR 231.1);
- Trade Mark Protection Act (SR 232.11);
- Designs Act (SR 232.12); and
- Patents Act (SR 232.14).

BE AWARE OF THE EXTRATERRITORIAL REACH OF THE EU AI ACT

The recently enacted EU AI Act applies to actors inside and outside the EU, as long as the AI system is placed on the EU market or its use affects EU citizens. The EU AI Act provides for a staggered date of application of its provisions:

- As of 2 February 2025, the prohibitions of AI systems deemed to present an unacceptable risk will already apply.
- As of 2 August 2025, the rules for so-called general-purpose AI models will apply.
- 2 August 2026 is the important date, as most of the remaining rules of the EU AI Act will then start to apply.
- As of 2 August 2027, certain obligations for high-risk AI Systems (embedded in regulated products) will apply.

The definition implemented by the EU is rather broad, capturing systems that are already in use. Therefore, if a Swiss company has any ties to the EU with respect to AI, it is advisable to carefully assess whether the new regulation is applicable. If so, the company must first determine its own role and secondly evaluate the risk category of each of its AI systems. These initial two steps will allow the company to assess the EU AI Act's legal implications on its business.

If a Swiss company has ties to the EU regarding AI, it is advisable to carefully assess whether the new regulation applies.

Different Roles and Risk Categories Lead to Different Obligations

As a first step, a company with ties to the EU with respect to AI should determine which role applies to it. The EU AI Act distinguishes between four different roles:

1. **Providers:** Natural or legal persons who (i) place their AI system on the EU market, (ii) put their AI system into service in the EU, or (iii) use the output produced by their AI system in the EU, are classified as providers, regardless of whether they are domiciled or established in the EU.
2. **Importers:** Natural or legal persons domiciled or established in the EU are classified as importers if they place an AI system on the market under the trademark of another natural or legal person domiciled or established outside the EU.
3. **Distributors:** Natural or legal persons who make an AI system available on the EU market without their activities qualifying for the role of a provider or importer are classified as distributors, regardless of whether they are domiciled or established in the EU.
4. **Deployers:** Natural or legal persons who use an AI system under their authority qualify as deployers, except if the AI system is used only for personal, non-professional activities.

The EU has adopted a risk-based approach: In a second step, each relevant AI system must be classified according to one of the four different risk categories defined in the EU AI Act: (i) unacceptable risk, (ii) high risk, (iii) limited risk, and (iv) minimal or no-risk.

As a result, AI systems with an unacceptable risk, such as practices that threaten fundamental rights (e.g., social scoring, individual predictive policing, or untargeted scraping of facial images), are prohibited under the EU AI Act. High-risk AI systems are subject to rules on their design, governance, and transparency, such as data governance, impact assessment and/or human oversight. AI systems that could have a negative impact on the security of people's fundamental rights (e.g., applications used to recruit employees or determine creditworthiness) fall under this second category. AI systems with limited risk, which may cause confusion or may be deceptive for users (e.g., chatbots or spam filters), are subject to transparency obligations. Minimal or no-risk AI systems (e.g., text generators) can be developed and deployed without additional legal obligations.

Violations of the EU AI Act can result in fines up to €35 million or 7% of total annual worldwide turnover (depending on which of the two figures is higher). There are exceptions to the applicability of the EU AI Act, such as scientific research and development as well as exclusive use for military or national security purposes.

Is the EU AI Act Relevant for You?

As the EU AI Act is a rather comprehensive piece of legislation combined with an extraterritorial reach, the possibility of falling into a prohibited or regulated category of AI varies widely depending on the company in question. Annex III of the EU AI Act provides a list of high-risk AI systems, including some sector specific use cases, which can help determine whether certain restrictions and obligations apply. Alternatively, there are several "EU AI Act Compliance Checkers" online that can be used to broadly assess one's risk category. These are not, however, officially provided by the EU but by independent organizations.

In practice, as an AI-deploying company, you can use the following questions to assess the applicability and impact of the EU AI Act:

1 Does Your System Qualify as an AI System?

Start by determining if your system qualifies as an AI system under the EU AI Act. The definition in Article 3(1) covers a broad range of systems. Check whether your software involves any form of automated decision-making or problem-solving that relies on artificial intelligence techniques.

2 Does Your AI System Impact the EU?

The EU AI Act may apply even if your business operates outside the EU. If your system is used or its output is consumed in the EU, you could fall under its scope. Evaluate whether your system is deployed in the EU or whether your services reach EU-based users.

3 Is Your System Exempt from the AI Act?

Not all AI systems are regulated under the EU AI Act. For example, systems used for exclusive military or national security purposes may be exempt. Review whether your system qualifies for any of these exemptions to avoid unnecessary compliance efforts.

4 Is Your AI System Prohibited?

The EU AI Act outright bans certain types of AI applications, especially those deemed harmful to society. These include systems that manipulate individuals subconsciously, exploit vulnerabilities, or involve social scoring, real-time biometric surveillance, or unauthorized facial or emotion recognition. Confirm that your system does not fall into these prohibited categories.

5 Does Your AI System Fall Under a High-Risk Category?

The EU AI Act classifies certain AI systems as high-risk, such as those used in critical infrastructure, education, employment, access to essential services, law enforcement, and biometric identification. If your system fits into any of these categories, it will be subject to stringent compliance obligations. Carefully assess if your AI involves any of these high-risk areas.

6 Do You Need to Comply with Transparency Requirements?

Transparency is key when AI systems interact directly with users or generate synthetic content. If your system produces audio, images, video, or text content that could be mistaken for real content (“deep fake”), or if it interacts with users (e.g., chatbots or virtual assistants), you need to inform users they are engaging with AI. Ensure your system complies with these transparency requirements to avoid penalties.

If, based on a first reading, the EU AI Act is potentially applicable to your company, we recommend a thorough assessment of the system as such, as well as of the legal obligations and implications according to the risk category into which your company‘s AI system falls.

PART 3: LIABILITY

Key Takeaways

In principle, AI-deploying companies are liable for AI output or actions generated by them just as if they had generated the output or acted without the use of AI. This means that AI-deploying companies are liable if they wilfully or negligently use AI tools so that it constitutes a breach of contract or tort, and if this AI use causes damage to others. Therefore, diligence is key when offering AI-powered services.

In the future, AI providers and, depending on the level of the AI tool customization, also AI-deploying companies may face strict (i.e., non-fault based) liability regarding injured individuals for personal or property damage as well as damage arising from corrupted or destroyed data. Most likely, over time, Switzerland will align its product liability legislation with pending new EU legislation. For the time being, providers are only exposed to such liability if they sell tangible products with AI embedded.

Some typical liability risks for AI use cases can be mitigated in the agreement with the AI provider (e.g., excluding the provider's right to use or sell data generated through your use of the AI tool).

Contractual limitation of liability with respect to customers is possible to the same extent that it would be allowed for any other means of contract fulfilment. Especially if limitation of liability clauses are contained in general terms and conditions, attention should be paid to their enforceability.

EXISTING LEGAL FRAMEWORK ON LIABILITY – WHAT APPLIED IN AN AI-FREE WORLD ALSO APPLIES TO AI

In Switzerland, damage caused by AI tools can lead to civil liability based on breach of contract, tort, or product liability (a specific kind of tort liability based on the Product Liability Act).

Contractual and Tort Liability

Without specific legal provisions, liability arising from the use of AI is governed by the existing legal framework in Switzerland. In plain terms, this means that what is not allowed without the use of AI is also prohibited when using AI. The focus of the following chapter is on potential liability issues for companies that deploy AI ("AI-deploying companies") and generate output with the AI-embedded applications, or let their customers generate output with it. Thus, AI-deploying companies are civilly liable for damage caused to others by use of AI tools if this use somehow constitutes a breach of contract or tort. Examples for torts caused by AI are violations of data protection and intellectual property rights, or unfair competitive behavior.

What is not allowed without the use of AI is also prohibited when using AI.

With a few exceptions, both contractual and tort liability are attributed only if the AI-deploying company willfully or negligently causes the contract violation or tort. Therefore, not only the employees of AI-deploying companies but also customers will have to learn to interact responsibly with AI tools (e.g., with large languages models ("LLMs")). For example, if customers provoke problematic AI output through their own unlawful input (in case of LLMs, the entered "prompt" by the customer), the deploying company should not be liable for this output, at least not if the software embedded in the AI tool contains reasonable measures to prevent unlawful output.

Other potential sources of faulty AI output lie in the development stage of the AI tool. Examples are its programming, the choice of data sets that the AI is trained on, as well as the duration of its training (AI

tools can be under- as well as overtrained). Most AI tools are "black boxes", meaning that beyond their original programming and training, humans do not know how the AI tools arrive at a particular output. This makes it difficult to anticipate their future behavior, and to prove a causal link between faulty output and a specific step during the development stage. In using such a black box mechanism, the AI-deploying company knowingly assumes a risk. Appropriate diligence is, thus, key in choosing the AI provider and the AI tool. Important aspects to consider are:

- the size of the training data sets: likely large and high-quality training sets are preferred;
- monitoring and update: choose an AI tool that is continually monitored and periodically updated by the provider.

In some cases, having an employee run AI generated output through an internet search engine to check for copyrighted texts or pictures or otherwise having an individual check AI generated output before it is released to third-parties can further reduce generative AI related liability risks. Whether such steps are useful will depend on the AI tool's particular task. Hence, this may be less relevant for a chatbot, whose purpose is reducing the need for human attention.

Additional liability mitigation tips to consider when setting up your contracts with AI providers or your customers will follow below.

Product Liability

In some cases, AI tools are first installed on tangible products or machines that are then sold or leased to companies (e.g., waiter robots at restaurants). Under such circumstances, the manufacturer of the product itself (= the AI provider) is directly liable for personal or property damage caused by a faulty product, based on the Product Liability Act. Product liability also pertains to those who substantially alter the product, which might include some AI-deploying companies ("quasi-manufacturers"). Due to the complexity and autonomy of AI, however, it may turn out to be difficult for an injured individual to prove that the AI was actually faulty.

It may still take several years until product liability in Switzerland also covers faulty software as such.

As of today, product liability is generally limited to tangible products. Yet, this year, the EU Parliament endorsed a revision of its Product Liability Directive, which extends product liability beyond tangible products to include software itself (thus including AI tools). Next to personal or property damage, it also covers damage arising from corrupted or destroyed data. In addition, the revised directive lowers the burden of proof for the injured individual to show defectiveness of the product or software and causality. Switzerland will most likely, and over time, adapt its Product Liability Act to reflect this revision. The revised EU directive still needs to be formally approved by the EU Council, and its provisions will, at the earliest, only take effect by the end of 2026. Considering this timeline, it may still take several years until product liability in Switzerland also covers faulty software as such.

CONTRACTUAL MITIGATION OF LIABILITY RISKS IN THE DEPLOYER–PROVIDER RELATIONSHIP

Before approaching potential AI providers, future AI-deploying companies should first identify their own pre-existing contractual and statutory restrictions that might expose them to liability if they launch an AI powered service. Some examples of potential restrictions are:

- the data the AI-deploying company wants the AI tool to process is covered by pre-existing non-disclosure agreements;
- the existing customer contracts completely prohibit the use of AI for specific parts of contract fulfilment;
- statutory data protection obligations; or
- professional secrecy laws.

Many of the liability risks thus identified can be addressed in the agreement with the AI provider. Most AI-deploying companies will want to restrict or

exclude rights of the provider to use (e.g., as training data) or even to sell data generated through their use of the provided AI tool. To comprehensively secure the data, it might prove helpful to have also the provider (with its subcontractors) enter into a non-disclosure agreement and to oblige the provider to implement reasonable data security measures for its AI system. Another possibility to mitigate liability risks is through contractual indemnification clauses that oblige the AI provider to indemnify the deployer for third-party claims caused by its AI tool. As with insurance policies, however, attention should be paid to the extent of such an indemnification clause's coverage.

CONTRACTUAL MITIGATION OF LIABILITY RISKS IN THE DEPLOYER–CUSTOMER RELATIONSHIP

A typical way to avoid liability is by contractually limiting the AI-deploying company's liability from the outset. Under general Swiss contract law, contractual liability (but not product liability) can be excluded for slight and medium negligence. It cannot be excluded for gross negligence or intent. It is admissible to exclude, however, any contractual liability (except product liability) for subcontractors to whom contract performance is lawfully delegated. Here, the principal cannot be held liable later if the subcontractor uses AI tools to perform the contract in a way that breaches the contract. Please note that negligence or intent are judged at the level of the AI deploying company, not at the level of the AI tool, which is not recognized as a person

Limitation of liability is often dealt with in general terms and conditions ("GTC"). Please be aware that the enforceability of such clauses may depend on how carefully they were drafted. For example, limitation of liability clauses in GTC should be highlighted visually (e.g., by using bold letters and a bigger font size) and should explicitly state the extent to which liability is excluded, rather than simply referring to the applicable provisions of the law. In a business-to-business context, consider instead addressing liability in individually negotiated agreements with the customer itself (or to specifically refer to the GTC clause excluding/limiting the liability in the agreement or an order). In a business-to-customer context, GTC clauses that create an unfair imbalance of the rights and obligations of a consumer are unenforceable. Therefore, the extent to which liability can be legally limited for consumers depends on the overall arrangement of their contractual rights and obligations.

As of now, no specific rules exist in Switzerland for limiting liability of contract performance carried out by AI tools. If the AI-deploying company's contracts or GTC already contain clauses that generally limit liability, these clauses should also cover the future use of AI tools. Disclaimers that go beyond the limitations of contractual liability outlined above are not enforceable. Disclaimers or warnings can, however, still be useful in practice for managing customers' expectations – if applicable, in combination with disclosing that AI output is created automatically and not checked by a human prior to release (e.g., the output of a chatbot). Last, exposure to liability arising out of customers' interactions with the AI tool can be further reduced by contractually outlining in what way the customers are (and are not) authorized to use the AI tool. If such clauses are contained in GTC and limit the customers' rights considerably, however, also these provisions may be considered unenforceable.

PRACTICAL STEPS TO MITIGATE LIABILITY RISKS

Identify your Liability Risks

- pre-existing contractual obligations? (NDAs, AI bans)
- which statutory obligations apply to the intended AI use? (data protection laws, IP laws, competition laws, professional secrecy, product liability etc.)

Select (or Negotiate with) the Most Suitable AI Provider

- how reliable are the training data sets that the AI is trained on?
- exclude right of provider to use or sell data generated through AI use?
- NDA (including subcontractors)?
- obligation to implement data security measures for AI system?
- obligation to implement measures into software to prevent unlawful AI output?
- indemnification clause?

Set up the Contractual Relationship with Your Customers

- know to what extent disclaimers are (and are not) enforceable
- draft your GTC carefully (especially important clauses should be highlighted visually and worded clearly or, better yet, be included in the main agreement)
- disclose that you are using AI (especially recommended if AI generated output is not reviewed before release)
- contractually define how customers are authorized to use the AI tool and output

Before Releasing AI Generated Output to Customers

- ensure that your employees are trained to properly use the AI tool
- consider having humans check AI output for violation of IP rights, data protection rights etc. before release to customers or the public

PART 4: DATA PROTECTION

Key Takeaways

The processing of personal data by companies operating in Switzerland – also in context of AI applications used by such companies and individuals – must comply with all applicable data protection laws.

Many aspects to consider from a data protection perspective are not particular to AI applications. Given the amount of potential personal data involved, however, the AI context increases the relevance of data protection law.

Besides technical measures, when it comes to data protection, the proper training and inclusion of employees in AI projects are essential.

INTRODUCTION

With the rapid advance of digitalization in recent years also came an increase in digitally available data. Thanks to "Big Data" technologies, the analysis of data previously limited to a company's own data warehouse can now be expanded to almost infinite amounts of data from an almost infinite number of sources.

When faced with this data abundance, many companies fall back on AI to improve efficiency: AI's machine learning capabilities make it easier to process massive and highly complex datasets, identify patterns, develop detailed insights, and filter out very particular information from deep inside the ocean of Big Data. Thus, companies believe that these solutions will allow them to make faster and more accurate decisions, anticipate market and industry trends, analyze customer behavior, optimize, and personalize digital marketing as well as raise their business performance and efficiency overall to carve out a competitive edge.

The processed data often includes "personal data", meaning any data referring to identifiable individuals (the "data subjects"). Some examples of personal data are a person's name, address, date of birth, sex, gender, telephone number, bank account details, IP address, license plate number, and location data.

In this context, the processing of such personal data – meaning any relevant handling of data, including the training, fine-tuning, or prompting of the AI – regularly raises questions and concerns about data protection. It remains, however, important to remember that not every type of data automatically is personal data and, hence, there may be certain AI applications or processing activities that do not fall under data protection legislation. The latter may be the case where such AI applications only process factual data or anonymized or (arguably) pseudonymized data. While this delineation will continue to be discussed and developed, the focus of this contribution lies on solutions that process personal data, for example, in the context of the input received or the output created and used.

It remains important to remember that not every type of data automatically is personal data.

Most companies in Switzerland process large quantities of personal data on a regular basis, and with the introduction of AI applications this amount will only increase. It is therefore crucial to understand what risks are associated with the use of AI in terms of data protection and how a company can appropriately avoid and/or manage these risks. While many data protection pitfalls arise irrespective of AI, some are more prominently connected to its deployment.

DATA PROTECTION CHECKLIST FOR THE USE OF AI

If a company chooses an AI application, either internally as an "auxiliary" for employees (e.g., ChatGPT) or externally as a tool in customer service (e.g., digital sales assistant chatbots on a company's website), the company bears responsibility to ensure data protection. For Swiss companies operating beyond Swiss borders and processing the personal data of natural persons outside of Switzerland, in addition to Swiss data protection laws, other data protection laws may apply (e.g., the data protection laws of the EU).

Especially, the deployment of a sales assistant chatbot may involve extensive collecting and processing of personal data, as the AI application relies on personal data to effectively work, understand what the customer wants, and, thus, answer requests or make targeted offers. A chatbot may not only receive information on, for example, age, gender, or addresses, but beyond such basic information potentially also personal preferences and users' moods and any other piece of information a user decides to share with such chatbots.

The following set of questions intend to help a company avoid and/or manage data protection risks with a particular focus on AI.

Question 1: Do You Inform Your Employees and Customers That Their Data is Being Processed?

Data subjects, such as employees and customers, have a right to be informed about the processing of their personal data, irrespective of whether this data is processed in context of AI. Usually this is done in the form of a privacy notice. As a minimum, a privacy notice must include (1) the company's identity and contact details; (2) the purpose of the processing; (3) where applicable, the recipients or categories of recipients to whom the personal data are disclosed; and (4) if the personal data are disclosed abroad, the country and, if such country does not provide for an adequate level of data protection, the guarantees taken to ensure their data protection, or the exception relied upon.

The company must inform the data subject regarding the processing of personal data both in cases in which AI applications are used by employees to process personal data as well as in cases in which the data subject themselves, as customers, use an AI application provided by the company. The law does not contain any explicit provision on any information obligation regarding the use of an AI application. Since customers, however, may not always recognize that their personal data is being processed by AI, for example, when chatting with a chatbot, the company is well advised to inform their customers that they are chatting with AI and not another human being.

Question 2: Does the AI Application Make Automated Decisions? If so, Do You Inform Your Employees and Customers About This Fact?

Certain AI applications may offer functions that qualify as automated decision making; for example, if a chatbot only grants relevant discounts or benefits to certain customers or presents different contract conditions based on the AI application's analysis. In such cases – in addition to its general information obligation – the company must inform the data subject about the fact, that a decision was made based solely on automated processing. This information is usually also included in the privacy notice. The data subject has the right to request the review of this automated decision by a human being.

Question 3: Did You Implement a Record of Processing Activities, or Did You Update Your Record of Processing Activities?

If your company (1) has a total of 250 employees or more, (2) processes large amounts of sensitive personal data (such as data on ethnicity, origin, and race, religious beliefs, political opinions, sexual orientation, health, biometric or genetic data), or (3) engages in high-risk profiling activities, your company is required to list all data processing activities in a so-called "record of processing activities". Thus, even if your company has less than 250 employees and has, so far, not been subject to the obligation to have in place this record, the necessity for implementing of this sort of record might arise due to the deployment of an AI application. Whether this is the case, must be decided on a case-by-case basis and ultimately depends on the functionalities of the AI application.

Question 4: Did You Carry Out a Data Protection Impact Assessment ("DPIA") Before Deploying Your AI Application?

Companies must carry out a DPIA if a planned data processing activity is likely to result in a high risk to the data subjects' personality rights. A high risk may, especially, arise in context of new technologies. A DPIA is thus a critical – and mandatory – self-assessment tool for companies when deploying an AI application, like a chatbot. If it follows from the DPIA that the risks of the planned data processing activity are, indeed, high, the data protection authority must be informed, unless the company has appointed a data protection officer and consulted them as part of the DPIA.

Question 5: Is Your Role and the Role of the AI Provider Clearly Defined in Terms of Data Protection?

If your company obtains AI as a service from an AI provider, you will likely assume the role of a controller, i.e., the person who determines the purposes and means of the data processing. The AI provider, on the other hand, will likely – and at least to a large part – assume the role of a processor, i.e., the person who carries out the data processing on behalf of the controller.

As the data controller, the company must ensure that the AI provider, as the data processor, processes the personal data in compliance with data protection laws and according to the company's instructions. In particular, the company must oblige the AI provider to ensure data security. Therefore, it is mandatory by law that the company enters a so-called "data processing agreement" with the AI provider. This agreement should include provisions on the technical and organizational measures that this AI provider must take to ensure data security. In practice, this data processing agreement will likely be included in the general terms and conditions of the AI provider.

Question 6: Is the AI Provider Located Outside of Switzerland/the EEA/the UK?

Where the processing of personal data is transferred to a processor located outside of Switzerland, the company must assess whether this processing occurs in a country that, according to the Federal Council's decision, provides for an adequate level of data protection. This can generally be assumed for the countries in the EEA and the UK. If this is not the case, the company must ensure an adequate level of data protection through other measures. The most common way is by entering into the EU Standard Contractual Clauses ("SCCs") – a legal framework that can be included as an annex to the data processing agreement. Additional analysis on the effectiveness of those SCCs in foreign jurisdictions may be needed.

Question 7: Do You Apply Appropriate Data Security Measures?

AI applications are usually not isolated from your overall IT system. To comply with your data security obligations, appropriate technical and organizational measures must be taken to protect personal data against any data security breach. We suggest regularly testing the security of your systems. For this purpose, ensure that your servers and anti-virus software are up to date, perform regular penetration testing, and fix existing security vulnerabilities as soon as possible – the same as you would for your other IT systems. As many data breaches can be attributed to weak or stolen passwords, ensure that your employees use strong passwords and do not leave their computers unlocked when unattended, especially when working remotely, as well as enforce two-factor authentication. Wherever feasible for the use case, personal data should be anonymized, pseudonymized, or encrypted.

Question 8: Do You Know How to React in the Event of a Data Breach?

With a data security breach – for example, a cyber-attack that leads to the loss of personal data – a company is obliged to notify the data protection authority of this incident, provided that such a data security breach results in a high risk for the personality of the affected data subjects. Moreover, a company is obliged to inform the affected data subjects of this breach if it is necessary to protect the affected data subjects (e.g., they must change their passwords) or if the data protection authority requires it. Given that through AI applications, specifically with chatbots, potentially large amounts of customers' personal data are collected and processed, it is not unlikely that the loss of such data would meet the threshold of "high risk" and

a notification obligation may arise. If an obligation arises, the company must inform the data protection authority as soon as possible. Needless to say, in case of a data breach, mitigating measures should be deployed wherever possible.

Question 9: Are You Able to Answer a Request for Information? Are You Able to Provide Sufficient Information on the Logic of the AI's Decision Making?

If an employee or customer requests information from the company as to whether personal data relating to them is being processed, the company must be able to provide such information within 30 days. As a minimum, the company must inform them about (1) the identity and contact details of the company, (2) the processed personal data as such, (3) the purpose of the processing, (4) the retention period of personal data, (5) where applicable, the recipients or categories of recipients to whom personal data are disclosed, and (6) if the personal data are disclosed abroad, the country and, if such country does not provide for an adequate level of data protection, the guarantees taken to ensure such data protection, or the exception relied on.

On top of the above – which is specific to AI applications subject to automated decision-making – an employee or customer also has a right to obtain information regarding the reasons for the AI application's decision allowing them to comprehend and review the AI decision. The company must therefore provide the data subject with information on the decision-making criteria and personal data which the decision was based on. In practice, this can be a major challenge for a company due to the black-box nature of many AI applications. In many cases, the company will be dependent on the cooperation of the AI provider to acquire the necessary information to fulfil its information obligations under data protection law. This should be taken into account when concluding the contract with the AI provider.

Question 10: Do You Ensure That Only Data Is Collected That Is Necessary to Achieve the Communicated Purpose?

To analyze customers' personalities and purchasing behaviors, companies have an interest in collecting as many personal characteristics about their customers as possible. However, when processing personal data, they are bound by the principles of proportionality and purpose limitation. Following these principles, the collection of personal data must be minimized to such personal data that is required to achieve the intended purpose(s) of the processing. The company must therefore – before collecting such data – assess which personal data is necessary for a specific processing purpose (e.g., marketing activities).

It goes without saying that in context of AI applications, such as a chatbot, companies will often not be able to fully control the personal data the AI processes, since it is the customer as user of the AI application who decides what personal data they share with the AI application. It is therefore advisable to request your customers limit the personal data they provide to the extent required as well as regularly audit customers' data storage and delete personal data that is no (longer) needed.

Question 11: Do You Spread Awareness on Data Protection Among Your Staff?

It is crucial to properly instruct and train employees to treat their own personal data and the personal data of their co-employees and customers with the appropriate care and in compliance with data protection laws. Employees should be trained to be careful with the information they use as an input for the AI application and to avoid using personal data whenever possible. Sensitive personal data should not be used at all unless the concerned data subject has given its consent to do so. Wherever possible, employees should only rely on anonymized data (i.e., data changed so that it can no longer be traced back to the data subject) or pseudonymized data (i.e., data encrypted so that only authorized people with access to the encryption key have access). As regards the output of an AI application, employees should carefully review if such output contains personal data, and if so, remove them before using the output, unless the concerned data subject has given its consent to do so. In any case, employees should ensure that the personal data contained in the output is correct.

Employees should carefully manage AI inputs and avoid using personal data whenever possible.

Question 12: Is There Anything Else You Can Do to Strengthen Data Protection in Your Company?

Appointing a data protection officer would be a useful asset for the company when it comes to data protection governance in the context of critical data processing activities involving AI. A data protection officer serves as a first point of contact for data subjects and authorities and takes over the important task of training and advising the company and its employees in data protection matters.

Last, it is generally recommended to establish internal processes, data protection policies, and action plans to ensure compliance with data protection requirements, particularly around the internal use of AI applications. On the technological level, IT solutions can be implemented for the controlled deletion of personal data when it is no longer needed, reducing the risk of data breaches, and simplifying compliance. In the event of a data breach, action plans with clear step-by-step instructions, and checklists come in handy.

Through a combination of the above outlined measures, companies can adequately respond to data protection hazards and manage risks in connection with the deployment of AI-based applications such as chatbots. On top of that, having appropriate data protection governance in place will not only limit the risk for (data protection) liability, but also strengthen the trust of clients, customers, and other stakeholders, resulting eventually in a competitive advantage on the market.

Having appropriate data protection governance in place will not only limit the risk for liability, but also strengthen the trust of clients, customers, and other stakeholders.

PART 5: INTELLECTUAL PROPERTY

Key Takeaways

Using generative AI applications which are trained, fine-tuned, or prompted on IP protected content may infringe third-parties' IP rights and bear liability risks for the user of a generative AI application.

Currently, generative AI cannot be the author of a work of art or the inventor of a technical invention.

It is unsettled yet to what extent a user of AI applications can be considered the author of a work result generated with a generative AI system based on their prompts. At least in cases in which the AI application is used as a mere tool in an overall process and a human had sufficient influence on the result, the output could potentially be subject to IP protection. For most cases, however, works created with generative AI applications will not be accessible to IP protection.

To mitigate the risks of third-party IP infringements, to protect the company's own IP rights, and to avoid inadvertent disclosure of trade secrets and other business-related confidential information, it is recommended that a company carefully reviews the general terms and conditions of the AI provider, especially with regard to the use of the company's data for training purposes and the ownership in any work results, created by the AI application.

AI is a great technology for generating first ideas and assisting with subordinate aspects of work creations. However, it should be used with caution for the creation of final work products, especially when it is key to claiming exclusive rights in such work products.

Internal AI policy guidelines as well as appropriate instruction and training of staff members are pivotal to a responsible use of AI in connection with IP protected content.

INTRODUCTION

Currently, many companies are adopting AI to generate content and by doing so, often rely on so-called generative AI applications like ChatGPT and Microsoft Copilot. These applications are able to create text, computer code, images, audio and video content in response to their user's prompt. To receive such output, users can – within their prompts – "feed" the AI application not only text, but also computer code, images, audio and video content. With these AI applications, opportunities come along, but also significant legal risks, especially with regards to the protection and infringement of intellectual property rights.

Intellectual property ("IP") refers to intangible creations, such as creative works of art, trademarks, designs, and inventions. IP rights are intended to give means to their holders to prevent or control the use of their IP by others. This naturally also applies to the use of IP protected work results in connection with generative AI applications.

INFRINGEMENTS OF THIRD-PARTY IP RIGHTS

Before generative AI applications can be used, they must ingest enormous quantities of training data. This data may also include IP protected content. Once trained, the AI can then generate "new" content, based on the ingested data. If, for example, asked to create a poem or a new brand name the AI application draws on pre-existing and potentially IP protected corresponding content for reference. IP can also be included in the prompts entered by a user, be it the user's own IP rights or third-party IP rights. The training and the use of generative

AI applications can thus potentially amount to an infringement of third-party IP rights, if the IP protected content used to train, fine-tune, or prompt the AI application was not licensed for such purposes. Similarly, there is also a risk that the AI "plagiarizes", i.e., produces outputs that incorporate or are otherwise derivative of protected content with no significant changes to it. Generally, when used in a commercial context, the more the output resembles the IP protected content, the more likely it is to constitute an infringement.

Where the AI has been trained on IP protected content, users might face allegations of IP infringement if they use the outputs in a commercial context. The liability for IP infringement does not depend on the intention or knowledge of the infringer. Likewise, if IP protected input belonging to a third-party is used by the generative AI application to further train the system, the user could potentially be made liable for contributory IP infringement with respect to the training of the application with this third-party content and future results created by the generative AI application. It is therefore recommended to refrain from uploading third-party content into a generative AI application without previously making sure that the system will not use such content for its further training, in particular by checking the applicable terms and conditions of the generative AI provider.

Infringement of Copyrights

In the context of the use of generative AI applications, the infringement of copyrights is the focus.

Copyright law grants the creator (i.e., the "author") of a work of art (such as a painting, a photograph, a song, a code) exclusive rights regarding the use of such work. Particularly, the author alone decides on how, when, and by whom their work is used and is entitled to determine whether their work can be copied and whether these copies may be reproduced. This exclusive reproduction right also includes the digital copying of a work. Uploads and downloads or the storage of a work on a data carrier are all considered reproductions.

During the training of generative AI applications, in particular when creating the training data set and during the training, technical reproductions of entire or parts of copyrighted works may be made. Similarly, a digital copy of a work is created when the work is used as a prompt or to fine-tune. If the copyright holder of the relevant works has not consented to such use of their works, these actions may qualify as infringement of their exclusive reproduction right.

While the author's exclusive right is generally subject to certain exceptions, none of the exception provisions under current copyright law grant a comprehensive justification for the use of copyright protected works with generative AI in the commercial context. As examples, data sets created when training, fine-tuning, and prompting generative AI usually do not meet the criteria for temporary or accompanying copies, and the scientific exception only allows the use of copyrighted works for training, fine-tuning, and prompting, if these acts are carried out for the main purpose of scientific research. And this is rarely the case.

PROTECTION OF WORK RESULTS CREATED WITH USE OF GENERATIVE AI APPLICATIONS

Some companies may have an interest in protecting "their" work results generated with help of generative AI applications. Since the concept of most IP rights has originally been designed to protect intellectual creations of humans, however, whether IP rights can or should be available to the outputs of generative AI is a hotly debated topic.

Protection of Copyrights

To qualify for protection under copyright law, a work must, among other things, be intellectual in the sense that it originates in the mind of the human author. While AI has admittedly been trained by humans, and while its algorithms are very complex and simulate to some extent the human brain, their direct output is – according to the current legal doctrine – generally not considered the result of a natural human's creative effort.

However, the question arises whether, in certain cases, the user of a generative AI application could be considered the author of a work considering the user's (creative) prompts. At least in cases in which the AI application is used as merely a tool in an overall

creative process, and a human had sufficient creative influence on the result, the output might be subject to copyright protection, whereby the user and not the AI application itself would be considered as author.

However, there is currently significant legal uncertainty regarding the copyright ownership of the final creation. One could also argue that other than the user of the AI application, also the person who programmed the underlying algorithm of the AI application, who trained the AI, or who provided the input data for the specific project, could be considered as (co-) authors of a work and therefore be granted protection under copyright law.

Protection of Inventions

For inventions, similar considerations arise as for copyrights. As a matter of fact, generative AI has already been used to help with new inventions, for example, in drug design. However, at least to the extent where the core inventive contribution was made by the generative AI system, most patent offices and courts abroad have so far rejected patent applications for inventions created by AI because patent laws require a human inventor to be listed on a patent. Hence, the same reasoning applies for the refusal of copyrights for works created by generative AI, namely that the original purpose of patent law is to foster human innovation by rewarding human intellectual efforts. How an AI application can be considered as a contributor to a patented invention, if at all, is currently uncertain.

The original purpose of patent law is to foster human innovation by rewarding human intellectual efforts

Based on the above, it might seem intuitive to not indicate the AI as the inventor on a patent application, but instead the "human using the AI". Similarly, as to the discussion with respect to copyrights, this approach might work where the AI application was used as a mere tool by the inventor. However, the discussion is more complex with patent law. The use of generative AI does not only impact the question whether patents for inventions made with these tools are accessible to patent protection at all, but also regarding the question how generative AI applications are to be considered in the analysis of the inventive step.

Given the lack of legal certainty in this respect, it seems, for the time being, advisable to protect core inventions primarily made by AI in the form of trade secrets and know-how, rather than by applying for patent protection and risking the disclosure of the invention without any appropriate reward.

Contractual Limitations to Obtaining Ownership in Work Results Created with Generative AI Applications

Even if a work result, created using generative AI, is not subject to intellectual property protection, there may be contractual provisions (usually in the general terms and conditions ("GTC")) between the provider and user of an AI application that govern the use of the work product. These GTC could, for example, foresee assigning ownership of any content created by AI to the AI provider. This would mean that the AI provider can freely use the work results created by the user of this AI application. This might be disadvantageous to the user's business interests. By contrast, other AI providers, such as OpenAI, have in their current GTC opted to assign rights to the output to the users, or make such assignment subject to certain conditions, for example, by stipulating that the role of the AI application, in creating the output, is clearly disclosed. This assignment of rights to the user of an AI application is, however, only possible to the extent it was "fully" created by that user and no third-party IP rights are infringed. Evidently, the GTC cannot transfer any third-party IP rights to the user, and any provision therein stating otherwise would not be enforceable.

TRADE SECRETS AND OTHER CONFIDENTIAL INFORMATION

In addition to the danger of infringing third-party IP rights, there is also a risk that businesses are inadvertently disclosing trade secrets or other business-related confidential information when using, training, or prompting generative AI – be it their

own trade secrets or third-party trade secrets. As mentioned, user prompts may be saved and used by the AI provider to improve their tools. If trade secrets or other business-related confidential information is used as part of a prompt, potentially not only can the application provider acquire a copy of this information, but the trade secret or confidential information may also become part of the AI application, and thus be included in some form in the output of other users. In other words, trade secrets and confidential information are at risk of being shared with the AI provider or even publicly with other users. In addition, this use puts the trade secret or confidential information at an increased risk of being hacked and/or leaked to third-parties. Finally, disclosing third-parties' trade secrets to other third-parties may even lead to criminal liability. As a result, we strongly recommended to either refrain from feeding generative AI applications with confidential content or to first consult the applicable terms and conditions to ensure risks cannot arise.

We strongly recommended to refrain from feeding generative AI applications with confidential content.

RECOMMENDATIONS

Still, there are many open questions both regarding the possibility of obtaining IP rights when generative AI applications are used and relating to the risks of infringing third-party IP rights or violating confidentiality obligations. As such, caution is demanded when using generative AI applications in this context.

In particular, companies should keep in mind the following:

- **Ownership of training data.** Consider using generative AI applications that have been solely trained on data belonging to the AI provider and/or the company itself, the public domain, or which have been, by third-parties, appropriately licensed to an AI provider.
- **Ownership of output.** Be aware that you will likely not be able to claim IP rights in the work results obtained by using generative AI applications. Hence, where exclusivity is key to your business purposes, human creativity is still demanded. In any event, review the GTC of a generative AI provider regarding ownership of the output and any IP rights related thereto, and ensure that you are entitled to (exclusively) use all work products created though the AI application.
- **Information used for prompting.** Be cautious with the information you use as an input for the AI application, and avoid using information that either:
  - is protected by IP rights of third-parties, which you are not licensed to use for this purpose

    or
  - constitutes a trade secret or other business-related confidential information.
- **Use of your data as training data.** Consider using generative AI applications that operate on a private cloud and check the settings on generative AI applications to see if they allow an AI provider to store and train on user's prompts. Whenever possible, seek appropriate (legal) protections and assurances against the use, storage, and training of the AI on the company's prompts to protect the company's trade secret and other confidential information.
- **Restraint in the use of (unmodified) AI-generated work results.** Limit the use of generative AI to business-internal use or to generate ideas, but not to create a finished work product. If you decide to use generative AI to create finished work products, run reasonable checks on such outputs for any IP infringements before using them commercially. Most AI applications have integrated tools to prevent IP infringements; however, currently these are not sufficiently reliable.
- **Internal compliance processes.** Put in place technical and practical safeguards (e.g., access limitations to certain AI applications, appropriate staff training and policies for use) to reduce the risk of producing IP infringing outputs and to prevent unintentional use of your IP protected works for further application training and, importantly, disclosure of trade secrets and confidential information.

PART 6: EMPLOYMENT

Key Takeaways

AI, with its immense data processing capabilities, is a useful tool to increase efficiency in operational processes. When data on job candidates or employees are processed, however, various labour law provisions must be considered before and during the deployment of AI.

The employer's AI applications may only collect and process data that concern the employee's suitability for the specific job or are necessary for the performance of the employment contract.

AI bias may reinforce human prejudices and cause AI applications to discriminate against certain employees. The employer must therefore keep a watchful eye on both the use of and decisions made by or based on AI.

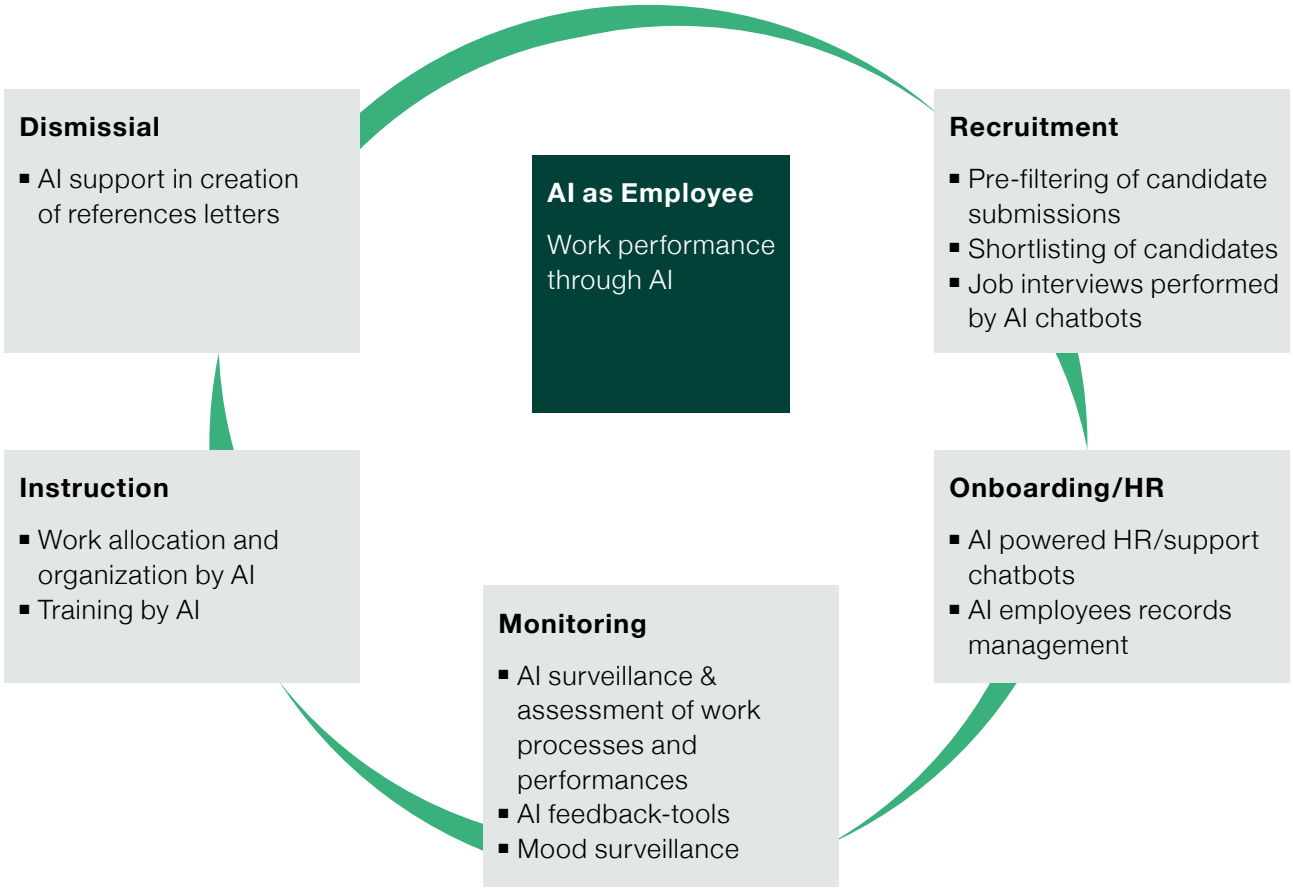
Under current Swiss law, employees have a right of co-determination regarding AI's use for monitoring purposes. To employees, however, introducing AI to the workplace brings many uncertainties and can cause them to be worried about its deployment. By involving the employees from the beginning and informing and instructing them properly on the use of AI applications, acceptance of, and trust in AI can be increased, and legal risks can be minimized.

INTRODUCTION: USE CASES FOR AI IN THE EMPLOYMENT CONTEXT

The rapid development of AI has a large impact on various aspects of the employment relationship. Indeed, AI applications can be used, and are increasingly being used for numerous purposes throughout the entire life cycle of employment relationships.

To name but one example, chatbot "Mya" by L'Oréal processes about two million CVs per year. Mya can process language, ask questions, and assess the answers to determine whether job candidates fit in well. During the ongoing employment relationship, AI applications can analyze work processes, monitor and analyze employee performance, or assign tasks to employees. Furthermore, AI applications can also be implemented in connection with dismissals. Of course, employees also use AI to perform their work services on their behalf.

AI has economic potential and brings various advantages for employers, for example, competitive advantages through talent acquisition, innovation, higher efficiency, as well as performance and cost reduction. AI applications, however, can also pose a variety of legal challenges. This overview aims at sensitizing employers to the various labour law related risks of deploying AI especially in the hiring and firing process and for surveillance, monitoring and instruction, and providing them with the necessary expertise to manage these risks.



CAN AI HIRE A JOB CANDIDATE OR FIRE AN EMPLOYEE?

AI can be a useful tool in people analytics, especially in the hiring and firing process, as it can process vast amounts of data, e.g., by filtering through CVs, scheduling and performing interviews, evaluating video or audio files, assessing emotions, analyzing behavior as well as movement quickly and – at least theoretically – making unbiased decisions based on facts alone. However, when using AI applications in the process of hiring new or dismissing current personnel, the employer must comply with various legal regulations.

Employer's Obligations Regarding Automated Individual Decisions

Switzerland does not prohibit automated decisions. According to Swiss data protection legislation, however, the responsible person must comply with specific obligations with decisions that (i) are solely based on automated processing of personal data and (ii) have legal consequences for the data subject or can otherwise significantly affect her/him. Such an automated decision is made when an AI application decides to (not) invite a job candidate to a job interview, (not) hire a job candidate or (not) terminate an employee and no individual subsequently reviews this decision.

In case of an automated individual decision, Swiss law requires the employer to actively inform the job candidate or employee about the process of automated decision making before or after such decision. The employer must also grant the job candidate or employee the right to present his/her opinion regarding the decision made. Finally, the job candidate or employee can demand that a human being review this decision (see also Part 4: Data Protection).

These obligations, however, do not apply if (i) the job candidate or the employee expressly consented to the automated decision making or (ii) the automated decision making is directly connected to the conclusion, or the performance of a contract and the job candidate or employee gets what he/she wants with said process. Thus, the employer need not comply with the aforementioned obligations towards the respective job candidate or employee if the AI application invites the job candidate to a job

interview, hires the job candidate under the requested conditions, or does not dismiss the employee.

Prohibition of Employment Discrimination

One of the original aims of using AI in the hiring and firing process is to make decisions free of human prejudice by disregarding criteria such as origin, age or gender. AI is, however, only as good as the data respectively the algorithm that applies. As the AI's algorithm is programmed by human beings, it can also reflect their errors and prejudices and – through repetition – reinforce them (so-called "AI bias"). Therefore, like human beings, AI can also make wrong decisions based on incomplete or incorrect data. For example, if an AI application is trained based on a male-dominated workforce, it learns to downgrade the ranking of job applications from female job candidates and ultimately rejects them, even though they might be better suited for the job in question.

An employer should therefore make sure that the AI application is programmed so that it does not make discriminatory decisions based on gender, ethnicity, age, or other protected characteristics.

The Swiss Equality Act protects employees thoroughly against discrimination based on gender. It prohibits not only direct, but also indirect gender discrimination. Indirect discrimination is given if a gender-neutral regulation results at a significant disadvantage for members of a particular gender. In exceptional cases, discrimination may be justified on objective grounds, for example if the gender itself is an essential characteristic of the advertised job. Consequences of a violation of the Equality Act are the right of the employee to bring a declaratory, injunctive and/or prohibitive action as well as damage payments up to six monthly wages, depending on the type and severity of breach. Notwithstanding the forgoing, the protection of employees against discrimination in Switzerland is relatively modest outside of gender discrimination. Switzerland has no general equality act under civil law.

Employers must ensure AI is programmed to avoid discriminatory decisions based on gender, ethnicity, age, or other protected traits.

Forbidden Job Interview Questions

If an AI chatbot conducts a job interview, the same rules apply as for a job interview by a human being: In principle, the future employer has the right to enquire and collect certain information about a job candidate to form an impression about his/her skills.

However, besides the data protection regulations that must be observed (for further information: Part 4: Data Protection), in Swiss labour law, Art. 328b CO in particular sets strict limits: The information collected and processed must always have a factual and direct connection to the specific job profile or position to be filled, or it must be necessary for the performance of the employment contract. The employer must therefore ensure that the AI is programmed so that it does not process information unrelated to the future employment relationship. AI applications that measure, for example, the heartbeat or facial expressions of the job candidate are generally not compatible with Art. 328b CO. Also, questions regarding, for example, family planning, sexual orientation, union membership or political opinions are generally off limits. The same applies to questions regarding a person's health situation, debt or criminal record, unless they are specifically relevant for the job or position to be filled. However, ensuring the latter is likely to be difficult. The AI application would need to decide on a case-by-case basis whether a question is permissible, but AI is usually unable to do this. Moreover, due to the inner workings of large language models, there is a high risk that AI will make decisions about a person's eligibility for a job based on non-employment information simply because the AI has learned that this information might correlate with specific character traits or skills required for that job. For example, it may find from its training that being a member of a soccer team goes hand in hand with having great teamwork skills or being a triathlete goes hand in hand with determination. Although this might be true, soccer team membership is not causal for good teamwork, and participating in triathlons does not tell you anything about the candidate's resolve. Both relate to a leisure activity. It is questionable, therefore, whether an AI application processing such information is compatible with Art. 328b CO.

If the data collected and processed exceeds the scope of Art. 328b CO, defined by the specific

employment relationship, this is considered a violation of personality rights. Due to the unilaterally mandatory nature of Art. 328b CO, the question of whether the job candidate's consent can justify this violation of personality rights is disputed in legal doctrine. The Swiss Federal Supreme Court, however, has affirmed that the job candidate's consent can justify a violation of Art. 328b CO. In any case, the employer must ensure that the job candidate has given his/her consent freely and only after being duly informed about the processing of his/her personal data by AI. Due to the imbalance in power in the employer-employee relationship, the standards for consent as a valid justification are rather high.

In case of a breach of Art. 328b CO, the job candidate has options for action, depending on the circumstances of the case. If the AI asks inadmissible questions during the job hiring process, the job candidate may refuse to answer or lie. In addition, the job candidate may be entitled to a damage claim or a compensation for pain and suffering.

AI Cannot Legally Engage or Dismiss an Employee

While automated decision making is not forbidden under Swiss law (see above), AI still cannot hire or fire an employee for the simple reason that it is not legally capable of acting in the sense of Art. 12 Civil Code. An AI application may decide and suggest that an employee should be hired or fired, but it must be the employer respectively the responsible natural person within a company who declares the intent to conclude or terminate an employment agreement.

CAN AI SURVEY AND MONITOR EMPLOYEES AND ISSUE INSTRUCTIONS?

In addition to the deployment of AI in the hiring and firing process, large companies increasingly use AI to analyze, evaluate, and optimize workflow and operating sequences. Usually, this is done by permanent observation and precise analysis of work performance, working conditions, and fluctuations in demand. Based on this observation and analysis, an AI application may also be able to directly issue instructions to employees. In this way, for example, the AI application assigns urgent tasks to the employee who can complete the task the quickest, considering his/her skill level and location.

However, heightened surveillance and monitoring in the workplace can negatively affect the health of employees. If productivity is continuously increased, employees may begin to suffer from stress because of elevated work intensity and limited autonomy in decision making. In extreme cases, this can lead to unsustainable and unlawful working conditions.

Proportionate Surveillance and Monitoring

When using an AI application to survey and monitor employees, the employer must observe Art. 26 para. 1 of the Ordinance Nr. 3 to the Swiss Labor Act on health care of employees in particular. This provision intends to protect employees from surveillance measures unjustified by operational or other recognized purposes, and hence it limits the use of surveillance systems that monitor employees' behavior in the workplace. Surveillance systems that are used to solely or primarily keep a sharp eye on employees are not allowed. In contrast, if the employer uses the surveillance system primarily for another legitimate reason (such as ensuring undisturbed operational processes, quality assurance, occupational safety, the optimization of work organization or the productivity of personnel), its use is permitted if the health and freedom of the individual employee is not impaired, and the employer uses the system proportionately to the intended purpose. Therefore, it is very important that the employer precisely determines the purposes of the AI application used, and based on this, defines the required scope of data.

Surveillance systems used solely or primarily to monitor employees are not permitted.

Furthermore, the employer's duty of care towards its employees according to Art. 328 CO and the requirements of Art. 328b CO regarding the collection of the employees' data also apply in the context of workplace surveillance and monitoring. The employer must therefore pay close attention to what data is collected from its employees and whether its processing leads to any form of unjustified

discrimination or violation of personality.

In addition, the employer must look out for provisions under data protection law that limit surveillance. The employer must therefore:

- carry out the employee surveillance and monitoring transparently, regardless of the means chosen;
- inform the employee comprehensively and in advance about the surveillance and monitoring;
- delete the gathered data after the shortest possible period of time; and
- exercise utmost caution and restraint when analyzing data from wearables in the workplace, such as fitness wristbands, data glasses or sensors that collect health-related information, because this information is considered particularly sensitive data within the meaning of the Swiss data protection legislation, whose collection and processing is subject to particularly strict data protection restrictions.

Involving Employees

As stated above, for transparency's sake, it is important that the employer provides its employees with comprehensive information in advance about AI applications used for monitoring them. In addition, employees have a right of co-determination ("Mitspracherecht"; but no right of co-decision) in matters of occupational health protection. AI applications that are used to survey and monitor employees are likely to be health-related and are therefore subject to the right of co-determination. The right of co-determination includes the right to be heard and consulted before the employer reaches a decision as well as the right to a statement of reasons for the decision if it does not or only partially hear the employee's objection.

Employees do not have a statutory co-determination right regarding the use of AI that goes beyond health protection. Before introducing AI in the workplace, however, the employer should examine whether any applicable collective bargaining agreement provides for employee participation regarding the integration of a new technology in the workplace (or generally restricts introducing AI).

Notwithstanding the foregoing, the employer must consider that there are many advantages of involving employees when it comes to deploying AI applications in the workspace: If employees are involved at an early stage, they can use their specialist expertise to assess whether the planned investments are sensible and expedient. If included from the beginning, employees will learn more easily how to use the AI applications correctly, but also how to improve the operation of the AI over time. For employees, the use of AI systems in the workplace is associated with many uncertainties but more involvement brings better understanding of the technology, and this will likely lead to an increase in trust and acceptance.

Involving employees in deploying AI applications in the workplace offers many advantages.

Finally, various parliamentarians and legal scholars consider the statutory participation rights of employees inadequate, particularly regarding the use of AI. In December 2023, a motion was put forward to strengthening participation rights of employees in the use of AI if it is used for recommendations, forecasts, decisions, etc. affecting employees or using employee data. Based on a mandate from the Federal Council to identify sector-specific need for action and possible options in connection with artificial intelligence, a legislative proposal is expected in 2025 (see Part 2: Regulation). Thus, a high likelihood exists that the legislative will propose an extension and reinforcement of employees' participation rights.

Instructions by AI

While it is possible and theoretically allowed under Swiss labor law to let AI give instructions to employees based on its surveillance and monitoring, the AI application must be programmed to comply with the prevailing legal order. The instructions must thus remain within the scope of what a human superior would be allowed to instruct. The AI application would have to decide on a case-by-case basis whether an instruction is permissible, but AI is – as mentioned above – to date usually unable to do this.

CAN AI ISSUE A REFERENCE LETTER?

If the employer enters the appropriate prompts regarding an employee's functions and responsibilities, performance, strengths and behavior into an AI application, it can generate a useful template reference letter. This template can be adjusted and made concrete with only little effort to fit the specific employee. However, the employer is not dismissed from its duty to ensure that all the information about the employee is correct, complete and benevolent. Furthermore, the employer is responsible for the reference letter not including any cryptic phrases that may sound good but contain hidden negative messages about an employee and other coding methods. Therefore, every reference letter generated using AI must be reviewed carefully.

Of course, data protection principles also apply in this context (for further information: Part 4: Data Protection).

Finally, the reference letters must be wet ink signed by a person who is functionally and hierarchically superior to the employee. Hence, while AI can be a useful tool in its creation, it cannot fully take over the process of issuing a valid reference letter itself.

CHANGE OF PERSPECTIVE: ARE EMPLOYEES ALLOWED TO USE AI TO PERFORM THEIR WORK SERVICES?

An employee's use of AI to perform work services is a highly debated topic. Questions especially arise with regards to liability (for further information: Part 3: Liability). In addition, the question arises as to whether employees are allowed to use AI at all considering the principle of personal performance. This principle says that employees must generally perform their work themselves (see Art. 321 CO).

The employer can and should decide whether and to what extent it provides its employees with a specific AI applicatlon and allows them to use it. The employer is allowed to permit the use of AI because the employees' obligation to perform their work themselves is non-mandatory and may be waived (see Art. 321 CO). Furthermore, the employer can also prohibit its employees from using AI. In this case, employees may not use AI to perform their work services. If they do so nevertheless, they breach their employment contract, which the employer can sanction under employment law, depending on the circumstances and the severity of the breach.

The employer can and should determine whether and to what extent employees are provided with and allowed to use a specific AI application.

If the employer does not regulate the use of AI, the situation becomes more complex: Subject to any other agreement or practice, employees must perform their work personally (see Art. 321 CO). It is unclear whether employees breach this obligation if they use an AI application for their work performance. In 2021, the Swiss Federal Supreme Court was confronted with the question of whether an algorithmic application can fulfil the legal concept of a substitute. A bank had used its algorithmic system to perform all execution actions necessary to provide financial services to its clients. The Swiss Federal Supreme Court concluded that the AI application could not act as a substitute as it does not possess legal capacity. Rather, the Swiss Federal Supreme Court considered the AI as a tool. Against this background, a breach of the principle of personal performance could be denied. The decisive factor for the question of whether employees are allowed to perform their work by using AI in the absence of an employer regulation is likely to be the extent to which the employees use AI. If the employee uses the AI's output without critically reviewing it, a breach of the employee's obligation of personal performance and due care is likely. Depending on the circumstances of the individual case and the severity of the breach, sanctions may include a warning, ordinary termination or, in rare cases, termination with immediate effect. However, if the employee critically reviews the AI's output and intervenes in the AI's result, if necessary, the use of AI should not constitute such a breach per se.

Glossary

The following glossary provides an overview of certain terms often used in the context of AI and applied throughout this Legal Guide. The definitions used herein mainly rely on applicable laws, including the EU AI Act and the Swiss Data Protection Act. Certain definitions (marked with an asterisk) are the (full or shortened) explanations as curated by the International Association of Privacy Professionals (IAPP) in its Key Terms for AI Governance, version of July 2024 (available at: https://iapp.org/resources/article/key-terms-for-ai-governance/).

Term	Definition
Accountability	The responsibilities of an AI system's developers and deployers to ensure the system operates in a manner that is ethical, fair, transparent and compliant with applicable regulations. Accountability ensures the outcomes of an AI system can be traced back to the entity responsible for it.(*)
AI application/system/tool	An AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.
AI deployer/user	A natural or legal person who uses an AI system.
AI distributor	A natural or legal person who makes an AI system available on the market and is not a provider or an importer.
AI importer	A natural or legal person who places an AI system on the market under the trademark of another natural or legal person outside the market.
AI provider	A natural or legal person that develops or has developed an AI system and places it on the market or puts the AI system into service under its own name or trademark.
Anonymization	Processing personal data in a way that the respective data subject is unidentifiable and re-identification is not possible (irreversible process).
Artificial intelligence (AI)	Artificial intelligence is a broad term used to describe an engineered system that uses various computational techniques to perform or automate tasks. This may include techniques, such as machine learning, in which machines learn from experience, adjusting to new input data and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers. It may include automated decision-making.(*)
Automated decision-making	The process of deciding by automated technological means without human involvement, either in whole or in part.
B2B	Business-to-business; transactions between businesses.
B2C	Business-to-consumer; transactions between a business and a consumer who is the end-user of the business products or services.

Term	Definition
Bias	In the context of AI, bias can arise in various forms, such as: ▪ Computational bias: Systematic errors or deviations in AI predictions due to flaws in data or modeling assumptions. ▪ Cognitive bias: Distorted thinking or judgment by individuals, which may inadvertently affect AI models. ▪ Societal bias: Systemic prejudices embedded in models through biased data or societal norms.
Chatbot	A form of AI designed to simulate human-like conversations and interactions that uses natural language processing and deep learning to understand and respond to text or speech.(*)
ChatGPT	A generative AI chatbot and virtual assistant developed by OpenAI.
CO	Swiss Code of Obligations (SR 220).
Copilot	A generative AI chatbot and virtual assistant developed by Microsoft.
Data controller	Data controller means a natural or legal person that, alone or jointly with others, determines the purpose and the means of processing personal data.
Data processing	Data processing means any handling of personal data, irrespective of the means and procedures used, in particular the collection, storage, keeping, use, modification, disclosure, archiving, deletion or destruction of data.
Data processor	Data processor means a natural or legal person that processes personal data on behalf of the data controller.
Data protection impact assessment (DPIA)	Assessment of data protection risks applied by data controllers when data processing is likely to result in a high risk to the personality or fundamental rights of the data subject.
Data protection officer	The data protection officer is the contact point for the data subjects and for the authorities, with the main task of training and advising the company in data protection matters and of participating in the implementation of data protection regulations.
Data security breach	Data security breach means a breach of security that leads to the accidental or unlawful loss, deletion, destruction or modification or unauthorized disclosure or access to personal data.
Data subject	A natural person whose personal data is processed.
Deepfake	Audio or visual content that has been altered or manipulated using artificial intelligence techniques. Deep-fakes can be used to spread misinformation and disinformation.(*)
EEA	European Economic Area.
Encryption	Security measure that translates data into a code that can only be read by people with access to a secret key or password.

Term	Definition
EU AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
Explainability	The ability to describe or provide sufficient information about how an AI system generates a specific output or arrives at a decision in a specific context.(*)
FADP	Swiss Federal Act on Data Protection (SR 235.1).
General-purpose AI (GPAI)	GPAI means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks and that can be integrated into a variety of systems or applications.
Generative AI	A field of AI that uses deep learning trained on large datasets to create content, such as written text, code, images, music, simulations and videos, in response to user prompts. Unlike discriminative models, generative AI makes predictions on existing data rather than new data.(*)
GTCs	General terms and conditions.
Intellectual property (IP)	Intellectual property refers to creations such as inventions, works of literature and art, designs, symbols, names and images used in commerce.
Large language models (LLMs)	A form of AI that utilizes deep learning algorithms to create models pretrained on massive text datasets for the general purpose of analyzing and learning patterns and relationships among characters, words and phrases to perform text-based tasks.(*)
Machine learning	A subfield of AI involving algorithms that iteratively learn from and then make decisions, recommendations, inferences or predictions based on input data. These algorithms build a model from training data to perform a specific task on new data without being explicitly programmed to do so.(*)
NDA	Non-disclosure agreement.
Personal data	Any information relating to an identified or identifiable natural person.
Profiling	Any automated processing of personal data with the purpose of analyzing or predicting certain personal aspects or the behavior of a data subject.
Prompt	Any input – such as a phrase, question, command or statement – into an AI application to cause a response or action.
Pseudonymization	Processing personal data in a way that it cannot be linked to a specific data subject without separate additional information (reversible process).

Term	Definition
Sensitive personal data	Data relating to ▪ religious, philosophical, political or trade union-related views or activities, health, the private sphere or affiliation to a race or ethnicity, ▪ genetic data, ▪ biometric data that uniquely identifies a natural person, ▪ administrative and criminal proceedings or sanctions, or ▪ social assistance measures.

AUTHORS

Christoph Lang
Partner Corporate

Sarah Drukarch
Partner IP & TMT

Andreas Lienhard
Partner Employment

Markus Winkler
Counsel IP & TMT and Financial Services

Simon Winkler
Associate Corporate

Carola Winzeler
Associate IP & TMT

Nicole Sutter
Associate
Employment

Myrtha Talirz
Associate Litigation

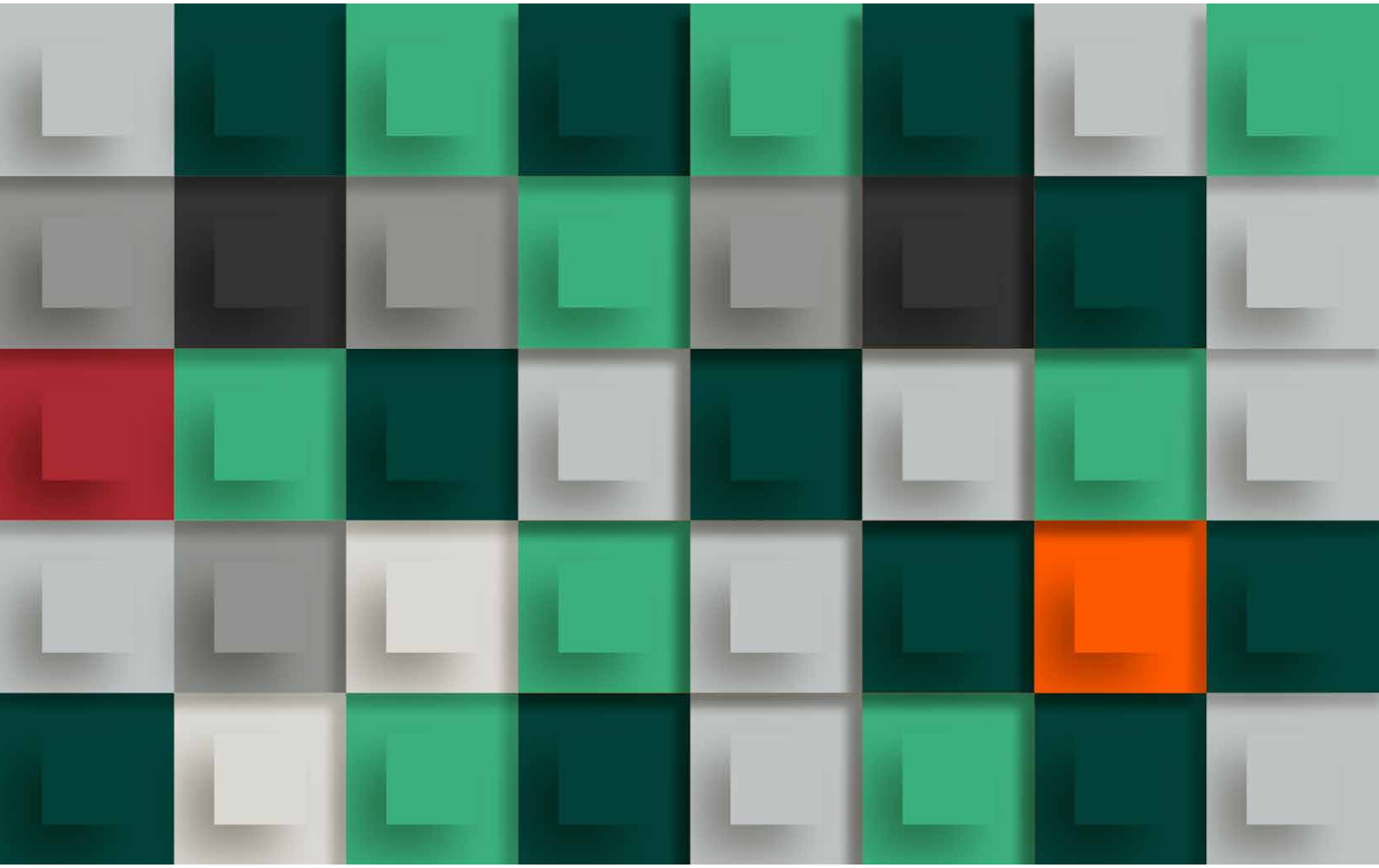
Luise Locher
Junior Associate
Corporate

Valerie Bühlmann
Junior Associate
Corporate and IP & TMT

DISCLAIMER

NO LEGAL OR TAX ADVICE

This Guide provides a high-level overview and does not claim to be comprehensive. It does not represent legal or tax advice. If you have any questions relating to this Guide or would like to have advice concerning your particular circumstances, please get in touch with your contact at Pestalozzi Attorneys at Law Ltd. or one of the contact persons mentioned in this this Guide.



This visual was created with AI and then reworked manually.

Pestalozzi Rechtsanwälte AG
Feldeggstrasse 4
CH-8008 Zürich
T +41 44 217 91 11
zrh@pestalozzilaw.com

Pestalozzi Avocats SA
Cours de Rive 13
CH-1204 Genève
T +41 22 999 96 00
gva@pestalozzilaw.com

pestalozzilaw.com