AI and Employee Data Protection in the European Union: 8 Key Takeaways for Multinational Businesses

Insights
12.30.24

Advancements in artificial intelligence and digitalization are changing the world of work at a rapid pace. In particular, when AI systems are used as workforce management tools, employers can automate a large number of tasks and optimize processes. However, in addition to bringing opportunities, these technologies also raise important legal issues – especially when it comes to employee data protection in a global environment. Notably, the European Union has some of the strictest data privacy laws in the world, which can impact your use of AI for employment-related decisions. We'll shed light on the impact of AI on employee data protection and discuss the legal requirements in the EU that must be considered when implementing AI systems. Here's what you need to know about workplace data protection and AI in the EU and 10 top takeaways for employers.

Key Points to Consider

- **Understanding the EU AI Act**: Employers should be familiar with the EU AI Act (which you can read about here) – especially since most workplace uses are considered "high-risk" categories and thus most highly regulated.
- **GDPR Data Protection Compliance**: Covered employers must comply with the EU's General Data Protection Regulation (GDPR) by ensuring AI systems comply with key principles, including transparency and data minimization, to avoid legal repercussions.
- **GDPR Human Oversight Requirement**: A specific section of the GDPR – Article 22 – notes that AI should assist, not replace, human decision-making in critical employment processes like hiring and terminations.
- **Discrimination Risks**: Organizations need to actively monitor and mitigate biases in AI algorithms to prevent discrimination.

AI in Human Resource Management

Artificial intelligence can be a great boost to employers' HR efforts. Here is just a sampling of the ways in which it can aid your workplace practices.

Recruiting Process. AI-powered tools can speed up the selection process by analyzing application data, conducting interviews with chatbots, and creating job recommendations based on historical

data. People analytics tools are often used to analyze the application documents with the help of machine learning methods.

Workforce Management and Process Optimization. AI systems are mainly used to automate routine tasks. For example, chatbots can be used to answer employee queries or to assist with administrative tasks, such as time tracking and vacation planning. The evaluation of work performance or the monitoring of absenteeism can also be automated by AI systems, which leads to an increase in efficiency.

Performance Tools. AI can be used to support workforce development with tools that identify individual training or development recommendations at an early stage. More employers are also using AI-powered employee retention and engagement programs to continuously improve their work environment and increase performance. Compliance with data protection requirements is particularly important in this area, as sensitive data on individual employees and development opportunities may be collected and analyzed.

AI in HR Risks

That being said, there are some critical risks that come along with using artificial intelligence for workplace-related tasks.

Discrimination Risks. Employers should use AI tools for recruiting with caution: Self-learning AI systems can pick up on and reinforce existing biases and biases in the training data, which can lead to discriminatory decisions. For example, if more male than female applications were positively evaluated in a training dataset, the AI system can conclude that men are better suited. This can lead to unlawful systematic discrimination against women.

Another problem is the so-called "black box" phenomenon. In the case of AI systems that make decisions independently, it is often not comprehensible how they arrived at a certain result. This creates risks for employers when they do not have precise knowledge of the underlying decision-making processes.

Employee Data Protection Risks. The use of AI in employee monitoring and evaluation can lead to data protection risks. Employers will need to be familiar with the GDPR's rules on processing personal data, particularly when used for monitoring purposes. Employers must ensure that the data collected is used only for the intended purposes and that the rights of employees are respected. Transparency and employee consent are also essential factors to consider when using AI systems.

Legal and Practical Considerations

There are several legal and practical considerations employers should take into account when it comes to the use of AI for workplace-related purposes – and the use of AI at work generally.

Handling Employee Data. Processing employee data, especially in connection with the use of AI systems, must be carried out in accordance with the requirements of the GDPR. Key principles include:

- **Purpose limitation**: The data collected may only be processed for the originally defined purpose. The data can only be used for other purposes with the express consent of the employee or based on a legal obligation.
- **Data minimization**: Only the data necessary for the respective purpose may be processed.
- **Transparency and consent**: Employees must be fully informed about the type of data processing, especially when AI systems are used. Consent is required in particular to process certain sensitive data.

The Impact of the EU AI Act. The EU AI Act regulates the use of AI systems within the European Union. For companies, this means that AI systems used in high-risk areas are subject to special requirements. The law takes a risk-based approach and distinguishes between AI systems with low, high, or unacceptable risk.

For human resources management and employee data protection, for example, AI systems can be used for the automated selection of applicants, for performance evaluation, or for monitoring employees. In these cases, employers must ensure that the AI systems work transparently and comprehensibly and that the rights of employees are protected.

The EU AI Act provides for strict sanctions if AI systems are used within an impermissible framework. Companies that violate the requirements of the law can be fined up to 35 million euros or up to 7% of the previous year's global turnover.

Mistakes When Using AI Tools. A common misconception among workers is that AI results are guaranteed to be error-free. But this is not the case. Even if AI is used as a work tool, the employee generally remains responsible for the results.

Secret Use of AI. Another liability risk arises when workers secretly use AI tools to complete their tasks. If, for example, an employee uses ChatGPT against explicit instructions from the employer without disclosing this, the question of responsibility arises. There could be a breach of contract here, especially if the use was not authorized. That's why it is important to set parameters and enforce your policies, as discussed below.

Creating Clear Guidelines

To minimize the legal risks associated with using AI in human resource management, you should consider creating clear guidelines for the use of AI systems. This includes:

- **Setting the parameters:** The use of AI should be limited to certain areas and processes of the company. It should be defined which AI systems may be used and under what conditions.
- **Training and educating employees**: Employees should be instructed in the use of AI systems to avoid mistakes and misunderstandings.
- **Employer's control obligations**: You should ensure that the AI systems function properly and monitor for potential discrimination or errors through regular audits and tests.

Data Protection Challenges and Solutions

Numerous data protection challenges arise when using AI in the workplace, especially regarding processing personal data. Key problem areas include:

- **Legal Basis for Processing Personal Data**. Under the GDPR, you must have a clear legal basis. This can be, among other things, the performance of a contract, the exercise of a legitimate interest, or the explicit consent of the data subject (Art. 6 GDPR).
- **Feeding AI Systems with Training Data**. AI needs training data to recognize patterns and make decisions. The question arises as to whether it is personal data or anonymized data. The consent of the data subject is usually necessary for the data protection-compliant use of training data.
- **Automated Decision-Making**. According to the GDPR, a data subject has the right not to be subjected exclusively to an automated decision that produces legal effects or significantly affects them (Art. 22 GDPR). This applies in particular to employment decisions, such as automatic application or termination processes. If the decision-making process is completely automated without human intervention, it is not permitted under the GDPR.
- **Data Protection Impact Assessment.** When processing large amounts of personal data, especially in connection with AI applications, a data protection impact assessment (DPIA) is often required (Art. 35 GDPR). This serves to assess risks to the rights of data subjects and to help take appropriate measures to protect them.
- **Big Data Analytics and Cloud Storage**. The use of big data analytics and storing data in the cloud increases data protection risks, especially when data is processed across multiple companies or countries. Cloud storage is now the standard and many products are no longer offered without it. This means data processing is generally not taking place on users' IT systems, but on servers, which are often located in different parts of the world.
- **U.S. Impacted By New Adequacy Decision of the EU Commission**. You should note that EU data protection standards are generally more robust that in the U.S., and U.S. business have certain obligations when transferring data to and from the EU. Following the failure of the earlier Privacy Shield and Safe Harbor agreements (Schrems I and II), which regulated the exchange of personal data between the EU and the U.S., a new EU-U.S. data protection framework was adopted in 2023. Under the new adequacy decision, personal data may be transferred from the EU to participating companies in the U.S. (based on Art. 45 GDPR for the transfer to third countries) that are certified according to the EU-U.S. Data Privacy Framework.

countries) that are certified according to the EU-U.S. Data Privacy Framework.

What Should You Do?

In order to ensure responsible use of AI in the workplace, clear guidelines should be developed and enforced. Here are some important provisions to consider including in your policies:

1. Select Specific AI Providers. Only select trusted and vetted AI tool providers to ensure that the technologies used are reliable and privacy compliant.

2. Restrict Use. Let employees know who can use AI and for what purposes.

3. Label AI-Generated Content. Ensure that all AI-generated content is clearly labeled so that its origin remains transparent.

4. Create Guidelines for Information Sharing. Define clear rules as to whether and under what conditions AI results may be passed on to third parties or received from third parties.

5. Address Potential Misuse. Create specific guidelines for the use of AI tools in areas such as image creation or software programming to avoid misuse, copyright issues, and unintended consequences.

6. Protect Trade Secrets. Clear rules should be put in place to protect trade secrets related to the use of AI.

7. Comply with Data Protection Regulations. Make sure all data protection regulations are observed, especially with regard to the processing of personal data by AI systems.

8. Designate a contact person for all questions regarding the use of AI.

Conclusion

To effectively manage the risks associated with AI use, organizations should develop policies that align with legal requirements and focus on the responsible use of AI while safeguarding employee rights. We will continue to monitor developments in this area, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions, contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our International Practice Group or our AI, Data, and Analytics Group.

Related People

Mauricio Foeth
Of Counsel
+52 55 48992148/+49 1575 8880464
Email

Service Focus

International

AI, Data, and Analytics