

THE DIGITAL INTERVIEW



AGNIESZKA ZWIERZYŃSKA, ADVOCATE AND SENIOR MANAGING ASSOCIATE AT ŁASZCZUK & PARTNERS, WRITES ABOUT LEGAL RISKS AND CHALLENGES IN USING AI IN RECRUITMENT.

Using AI-based systems, companies can optimize and automate the recruitment processes. However, along with bringing benefits, AI poses legal challenges that result from the newly adopted *EU Regulation 2024/1689* (AI Act), *EU Regulation 2016/679* (GDPR), and national regulations.

Recruitment agencies use AI, among others, for searching candidate databases, performing initial CV selection and probing the CVs of job candidates to find skills or experience that are interesting to the employer, assessing competency tests taken by job candidates, conducting recruitment interviews (chatbots) and helping prepare for the interview, by, for instance, summarizing information and refining the list of questions. AI systems also help survey data from various sources, such as social media profiles or the entire history of Internet activity related to the candidate, and minimize prejudices related to specific sensitive groups such as gender, age, race, and disabilities.

REGULATIONS

Recruitment agencies using AI systems should already have solu-

tions in place that are compliant with the General Data Protection Regulation (GDPR). With the AI Act, both regulations will most often have to be applied jointly as AI-based systems are used in recruitment.

Annex III to the AI Act lists AI systems used in the hiring and management of employees, including AI systems that "are intended to be used for the recruitment or selection of natural persons, in particular, to place targeted job advertisements, to analyze and filter job applications, and to evaluate candidates", among high-risk AI systems.

At the same time, if any form of automated personal data processing that results in a decision concerning an individual is used in recruitment, for example, to evaluate whether he/she is fit for the position, it is "an automated processing/profiling" within the meaning of the GDPR (Article 4(4) and Art. 22 of the GDPR). Thus, AI suppliers and users will often have to jointly meet the legality conditions specified for high-risk AI systems and profiling under the GDPR. In addition, the provisions of the Polish Labour Code should also be taken into account, regarding the scope of

data that can be processed in recruitment, in conjunction with the legal basis for this processing and information obligations towards candidates.

OBLIGATIONS

The AI Act imposes restrictions on the use of high-risk systems. The users are obliged to inform individuals that the decisions concerning them are being made with the use or assistance of a high-risk AI system. They also have to assign human oversight over high-risk AI systems to individuals with the necessary competence, training, and authority, as well as the necessary support. In addition, the users must inform the system supplier and the market surveillance authority if the system they resort to may pose a risk and suspend the use of the system in such a case. Keeping the logs automatically generated by that high-risk AI system, to the extent that such logs are under their control for at least 6 months, is another obligation.

The users also must ensure that input data is relevant and sufficiently representative given the intended purpose of the high-risk AI system and to the extent the

deployer of the AI system exercises control over the input data. The questions that immediately arise include whether every AI system used for recruitment is a "high-risk" system within the meaning of the AI Act. Do employers have to inform the candidates when they only use AI tools to search information from their databases more efficiently? And when should such information be provided?

The answer requires a detailed legal analysis of the specific AI system that employers use. The obligations for high-risk systems will enter into force on Aug 2, 2026. During the current adjustment period, employers should gauge the risks that stem from the AI systems they use.

GDPR AND PROFILING

Recruitment procedures involve the processing of personal data and must be GDPR-compliant. Obligations in this respect include, among others, having a legal basis for personal data processing—ensuring compliance with Art. 6 and 9 of the GDPR. In the case of job candidates in Poland, these are primarily labor law provisions, specifically Art. 22¹ of the Labour Code. Also,

EXPERT ARTIFICIAL INTELLIGENCE IN RECRUITMENT

consent may be required from job candidates for processing their data. They must be informed about the processing of their data. Articles 13 or 14 of the GDPR, put an obligation to provide a privacy policy or a similar GDPR information clause to a candidate.

AI systems are most often used for profiling, which produces legal effects for candidates. This brings into play additional GDPR-based obligations and requirements for the users of such systems.

According to Art. 4(4) of the GDPR, "profiling" means "any form of automated processing of personal data that involves the use of personal data to assess certain personal factors of a natural person, particularly to analyze or forecast aspects concerning the performance of candidates' work, their economic situation, health, personal preferences, interests, credibility, behavior, location or movements".

Anyone can object to having information machine-profiled by automated decisions if the result of the process has legal effects on them or significantly affects their lives. It is assumed that decisions

taken in an electronic recruitment process to offer a job opportunity to an individual, are decisions that "significantly affect" an individual (motif 77 of the GDPR). Thus, the candidates can object to using high-risk AI systems in their recruitment process.

However, the right not to be subject to decisions based solely on automated decision-making is subject to limitations. The GDPR allows for making decisions based on full automation, including profiling, when a decision based on automated decision-making is necessary for entering into, or the performance of, a contract between the data owner and the data controller.

AI is also allowed when the use of it is authorized by EU or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

AI may be used if the owner of personal data expresses explicit consent to it.

Employers who use AI systems for profiling and automated decision-making will have to decide if the conditions set out in the

GDPR are met. The safest way is to obtain consent from the data owner to the use of AI. If the employer can not get it, other options should be considered, such as, that the use of the AI system is necessary to conclude a contract with the candidate.

Moreover, an employer who uses AI for profiling and automated decision-making in recruitment should implement suitable measures to safeguard the rights and freedoms of the data owner and ensure his/her legitimate interests. This includes at least giving the candidates the right to "human intervention" by expressing their point of view and contesting the decision. Yet, this obligation does not apply to situations where automated decision-making is based on EU or local law.

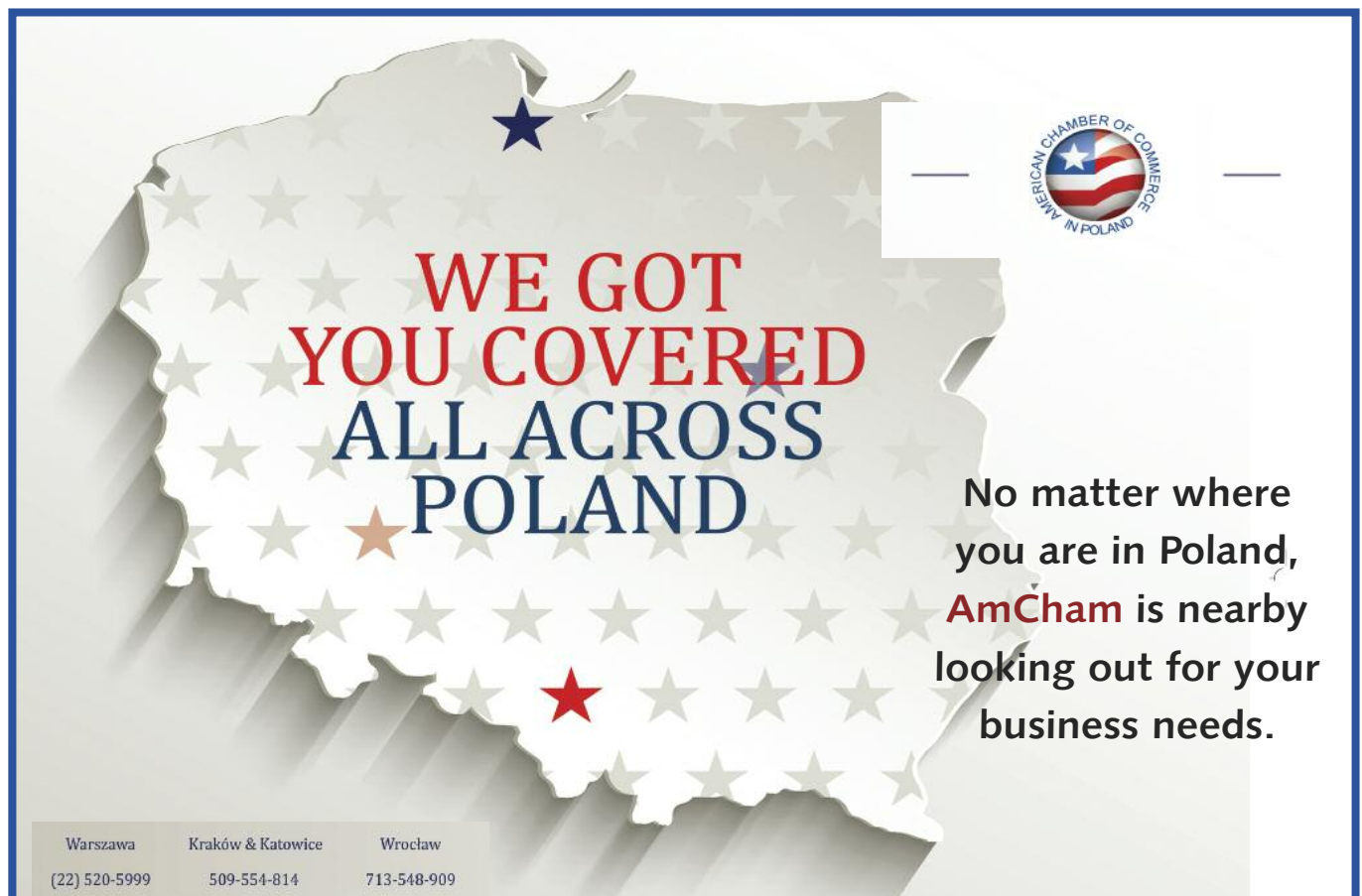
Additionally, if profiled by AI, the candidates should be informed about it. The employer must include relevant information in the privacy policy for job candidates. It must contain information about automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and potential conse-

quences of such processing for job candidates. In addition, the so-called Data Protection Impact Assessment (DPIA) of the effects of AI on data protection is necessary, in most cases.

WHAT TO EXPECT

The Polish legislator may introduce specific national solutions to the use of AI. The AI Act allows EU member states to introduce laws that are more favorable to employees in terms of protecting their rights through the use of AI systems by employers. It is not clear whether this will also apply to job candidates. It is not excluded that Polish regulators will issue more detailed guidelines. Certainly, the application of AI tools will require appropriate procedures, including those that specify the rules for the verification of AI-made decisions, as well as clear rules for the use of such tools and training for staff and management.

Documents within the scope of the GDPR should also be subject to revision, including privacy policies for candidates, a register of processing activities, and, in most cases, DPIA.



**WE GOT
YOU COVERED
ALL ACROSS
POLAND**

**No matter where
you are in Poland,
AmCham is nearby
looking out for your
business needs.**

Warszawa Kraków & Katowice Wrocław
(22) 520-5999 509-554-814 713-548-909

AMERICAN CHAMBER OF COMMERCE
IN POLAND