11.06.2024

Applicant Data Protection and Recruiting in Focus

Against the backdrop of digitalization and the increasing use of artificial intelligence (AI) in the application process, the protection of personal data is more important than ever. While developments are progressing rapidly, the need for advice is also increasing, which is why the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) is paying particular attention to applicant data protection as a sub-area of data protection.

The use of artificial intelligence has been established in the HR sector for years and its mass use is to be expected in the future. This makes data protection all the more important. Many things are possible in the application process, but there are clear limits that must be observed by controllers. An essential basic rule is that applicants (for an employment relationship) and persons whose employment relationship has ended are considered employees under data protection law (in accordance with § 26 (8) sentence 2 BDSG) and therefore have data protection rights comparable to those of employees. It is equally important that, due to the questions regarding the distinction between when an application begins and when a person can be considered an applicant, data controllers must consider and legally assess each individual stage of the application process separately.

Application documents contain a large amount of sensitive data, ranging from names, addresses and dates of birth to educational histories and information on previous employment relationships, as well as possible information on identification, origin, family and special categories of personal data such as trade union membership, severe disabilities or other illnesses. It is therefore of the utmost importance to treat this information with the same care and discretion as with employees. Special care must therefore be taken to protect the privacy of applicants and ensure compliance with data protection regulations.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg
Tel.: 040/42854-4040 | Fax: 040/42854-4000
E-Mail: mailbox@datenschutz.hamburg.de | Internet: www.datenschutz-hamburg.de

Hamburg

1 Current developments in employee data protection

On March 30, 2023, the European Court of Justice (CJEU) issued a ruling in Case C-34/21 that has a significant impact on the central legal basis of German employee data protection. This judgment raises doubts about the conformity and thus the applicability of § 26 (1) sentence 1 BDSG with regard to data processing in the employee context. The HmbBfDI was the first supervisory authority to comment on this ruling in a press release dated 03.04.2023 and called on both companies and the Hamburg legislature to re-examine the legal bases used. Despite the ruling, data processing operations in the employee context are not without a legal basis. In accordance with Art. 288 TFEU, the GDPR as an EU regulation and thus Art. 6 (1) (b)GDPR continues to apply directly in all member states as the legal basis for the processing of personal data for the performance of an employment contract.

This ruling has given new impetus to the ongoing political efforts to create a law on employee data protection. The Data Protection Conference (DSK) already called for the enactment of such a sector-specific law in a resolution on April 29, 2022. The creation of new regulations on employee data protection is also already mentioned on page 14 of the German government's coalition agreement. The mandate enshrined there is being implemented under the joint leadership of the Federal Ministry of Labor and Social Affairs (BMAS) and the Federal Ministry of the Interior and Homeland (BMI). As a first step, the BMAS and BMI drew up a joint paper at the beginning of the year with proposals from the two ministries on a total of twelve regulatory areas for an independent law, which largely coincide with the demands of the DSK.

2 Principles of the GDPR

When processing applicant data, the principle of lawfulness and fair processing (Article 5 (1) (a) GDPR), the principle of purpose limitation (pursuant to Article 5 (1) (b) GDPR) and the principle of data minimization (pursuant to Article 5 (1) (c) GDPR) apply. Both § 26 BDSG and Art. 6 (1) (b) GDPR are based on the criterion of necessity and stipulate that processing may only take place if it is necessary in order to perform, enter into or terminate a contract or employment relationship. In this context, the information obligations under Art. 13 and Art. 14 GDPR must also be observed. In

the practice of the HmbBfDI, there is an increased need for advice with regard to the information obligations, as these are often neglected or applicants feel insufficiently or not at all informed.

3 Definitions

Anglicisms are increasingly being used in the application process. Not every company means the same processing operations when terms such as recruiting, open sourcing, talent management or AI are used. Even if there are no uniform definitions for these terms, it is advisable to agree on a uniform use of language and, in case of doubt, always ask or inform yourself about which processing operations are taking place. The HmbBfDI understands the following terms as follows:

Recruiting refers to personnel recruitment or personnel placement and includes all activities aimed at filling vacant positions. This includes job advertisements, publications, interviews, signing contracts and onboarding processes.

Headhunters/talent scouts: Headhunting refers to the search for specialists and managers on a success basis, often on a contract basis and in particular using social media and business platforms.

Active sourcing refers to active recruitment, i.e. measures taken by a company to proactively identify potential applicants. In particular, candidates who are not actively looking for a job should also be reached.

Background checks/pre-employment checks are also known as applicant screening/candidate verification. These are checks that employers carry out to verify the information and background of candidates before hiring them, with third parties or via internet searches. It does not include security checks of employees in accordance with relevant security screening laws (e.g. SÜG and LuftSiG).

A **talent pool** is a database or online platform that contains profiles of applicants, employees, freelancers or other external contacts who may be considered for a position.

The terms **CV parsing/resume parsing** refer to the automated reading of applications (especially cover letters and CVs). The extracted data is then also automatically transferred to an application management system (BMS).

4 Phases in the recruiting process

The recruitment process can essentially be divided into different phases, ranging from the initial approach of potential candidates (cold calling) to the decision for (selection) or against (rejection) individual applicants.
In each phase, different activities take place, which are carried out by one or more parties and involve different legal relationships. For example, a person who merely views the careers page becomes an active applicant when they enter their information into the application form. If § 26 (1) sentence 1 BDSG no longer applies (see above), a distinction must be made using the necessity criterion of Art. 6 (1) (b) GDPR, regardless of whether the person is already an applicant or not.
In order to ensure a better overview and to meet the requirements of Art. 30 (1) GDPR, it makes sense to create an overview of all phases of the application process and the associated processing operations. It is not necessary to clearly delineate the individual phases. It is of course also possible for individual processing situations to occur in different phases. In this respect, the overview should not be understood as an exhaustive list. Such an overview could look like the example in Figure 1 and help those responsible to base the processing operations on the correct legal bases.

1 Phases in the recruiting process

5 Talent pools - inclusion only with consent

In principle, it is possible to be included in talent pools if applicants give their express consent. It is important that this consent is given completely transparently and voluntarily, taking into account the information obligations under Art. 13 GDPR. Consent should be given in text form and contain at least the following content

- Purpose of data storage in the talent pool
- Which data will be processed
- Duration of the storage
- Possibility to withdraw consent
- Information pursuant to Art. 13 GDPR
- Information pursuant to Art. 14 GDPR, if applicable

The information pursuant to Art. 13 GDPR can be integrated into the declaration of consent. In practice, challenges often arise in the area of the storage period of this data, especially when establishing an appropriate deletion period. It is important to note that consent is not valid indefinitely. In practice, it sometimes happens that consent is obtained, but no period is specified for the storage period. In the vast majority of cases, this means that the data is stored indefinitely. It is therefore recommended that consent is initially obtained for an appropriate period of time and that consent is requested again at the end of this period. If the data subjects do not respond, the

data must be deleted immediately and irretrievably. Different deletion periods may apply depending on the industry-specific requirements for the positions. Storage periods ranging from a few months to several years are therefore conceivable in individual cases. These depend on how long it would normally take to fill a corresponding position and are associated with possible time limits for legal action and exceptions in accordance with Art. 17 (3) GDPR.

6 Background checks are based on the right to ask questions in the job interview

As a rule, information about applicants can be obtained directly from them. The understandable need to obtain further information about them must be within the limits of data protection law. The conventional methods of getting to know applicants, such as job interviews, assessment centers, qualifications or job references, should be sufficient for this purpose. Even if internet research via search engines or the search function of social networks is not excluded per se, controllers must differentiate between the various networks. If information is obtained from third parties, the information obligations pursuant to Art. 14 GDPR must also be observed.

Not all information may be taken into account

Information that goes beyond the right to ask questions in the job interview may have to be disregarded (e.g. pregnancy, health data, political affiliation, Google headings). This also applies to information that has been obtained by chance or has become known in some other way. Within these areas, applicants should take care to present an appropriate image of themselves on social media due to the difficulty of providing evidence. In practice, it will often be unavoidable that a “chance find”, which may be inadmissible under data protection law, will work to the disadvantage of the applicant without the applicant concerned ever being informed of this fact.

Internet research - the purpose of the information disclosure determines its usability

If social networks and search engines are used, a distinction must be made between professional and private networks, as well as with regard to the purpose of the information disclosure. Private networks may not be used for background checks. It must also be taken into account that private information can also be disclosed in professional networks. A well-known example of a predominantly private network is Facebook, while LinkedIn is mainly used for professional

purposes. However, the transformation of these platforms and the associated differentiation according to the purpose of information sharing can be seen in platforms such as X (formerly Twitter), which is used for both professional and private purposes.

7 AI applications

From the publication of a job advertisement and the automated pre-selection of applicants to the analysis of job interviews and the use of chatbots, AI systems offer facilitation and automation options in the application process. The technologies available lead to data protection challenges. The HmbBfDI regularly receives inquiries about various software solutions, including CV parsers and emotion analysis. With regard to the use of LLM chatbots, the HmbBfDI published a checklist on November 13, 2023. This is intended to serve as a guideline for companies and authorities for the data protection-compliant use of chatbots. In addition, the DSK published guidance on the use of AI programs on 6 May 2024. This guidance is intended to provide an overview of the data protection criteria that must be taken into account when using AI applications in compliance with data protection law. It serves as a guide for the selection, implementation and use of AI applications.

CV parser - the processing options are decisive

Use is generally permitted if personal data is read out and transferred to an application management system in a structured manner. The principle of data accuracy pursuant to Art. 5 (1) (d) GDPR must be observed. If an additional data analysis is carried out after parsing, Art. 22 GDPR, which deals with automated individual case decisions, must be observed. In addition, the judgment of the European Court of Justice (CJEU) on Schufa of 07.12.2023 must be taken into account. According to Art. 22 (1) GDPR and the CJEU ruling, decisions with legal effect may only be made by humans. AI proposals that have legal effects for data subjects must be designed in such a way that the person making the decision has a genuine scope for decision-making and does not decide primarily on the basis of the AI proposal. Merely formal human involvement is not sufficient.

Emotion analyses - generally not permitted

Emotion analysis in the application process refers to the use of technologies that are intended to recognize and interpret the emotional states and reactions of applicants during the application process. This analysis can be carried out using various methods, including facial expression and gesture analysis, speech and tone of voice analysis or the evaluation of written responses. The aim is to draw conclusions about the applicant's personality, motivation and potential suitability.
Emotion analyses are problematic under data protection law in the application process because they are generally not necessary and the voluntary nature of consent could be questionable. It must also be checked whether biometric data is being processed (see also the DSK position paper on biometric analysis dated April 3, 2019).
In this respect, there is a synchronization with the AI Regulation, which lists the use of AI systems to infer the emotions of a natural person in the workplace (with a few exceptions such as medical aspects or safety aspects) as a prohibited practice in accordance with Art. 5 (1) (f) AI Act.

LLM chatbots - useful for job advertisements

AI-based systems such as large language models (LLM) and chatbots can take on a variety of tasks in the application process, such as formulating invitations or rejections, answering frequently asked questions, conducting initial selection interviews or providing information about the application process. The data protection-compliant integration of such LLM chatbots often poses data protection challenges for controllers.
Leaving a complete selection decision or a final candidate proposal to the LLM system is problematic from a data protection perspective and is generally not permitted. Such automated decisions must meet the requirements of Art. 22GDPR.

8 Outlook

The use of artificial intelligence (AI) in recruiting will continue to gain in importance in the future. At the same time, data protection requirements will also increase. In addition to the General Data Protection Regulation (GDPR), new regulations such as the European Union's AI Act and AI Regulation will play an important role. Companies are required to comply with strict data protection guidelines and implement transparent procedures.

The integration of data protection-compliant automated analyses may also have a positive impact on the entire recruitment process by enabling personalized, fair and non-discriminatory application procedures. The challenge here will be to find a balance between technological advances and the data protection of applicants. Controllers responsible should proactively address the requirements and implement the corresponding application options in compliance with data protection regulations in order to minimize legal risks, gain the trust of potential employees and applicants and strengthen their own public image.

Contact:

Eva Zimmermann
Phone: +49 40 428 54-4044
Mail: presse@datenschutz.hamburg.de