

PRZEGLĄD PRAWA ADMINISTRACYJNEGO

(7)2024 • DOI: 10.17951/ppa.2024.7.77-96

UNIVERSITY OF RZESZÓW

KATARZYNA HADY-GŁOWIAK

kglowiak@wp.pl

ORCID ID: <https://orcid.org/0009-0006-3038-5476>

UNIVERSITY OF ECONOMICS IN KATOWICE

STANISŁAW HADY-GŁOWIAK

stanislawhg@gmail.com

ORCID ID: <https://orcid.org/0000-0002-1060-6984>

Legal and Practical Aspects Concerning the Processing of Personal Data in the Recruitment Process

*Prawne i praktyczne aspekty dotyczące przetwarzania
danych osobowych w procesie rekrutacji*

Introduction

The recruitment process and the associated staff turnover are key areas where an employer should ensure compliance with the law, organizational and legal safety of processed personal data, which undoubtedly affects its professionalism and perception by external clients, such as job candidates. The standardization of the legality of this process is influenced by both national labor law regulations and EU regulations.

There is a consensus in the literature that the regulation of personal data protection issues by the EU legislator in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)¹ means that this act is applied directly and immediately in the legal systems of individual member states and introduces identical standards in all countries obliged to apply it. Furthermore, it is emphasized that “certain regulatory areas require some ‘decisional leeway’ and freedom in shaping legal solutions”²

The subject of this article is to identify good practices, occurring risks and irregularities in the processing of personal data of job candidates as part of the employee recruitment process and to develop principles for verifying the correctness of the functioning of this process as a tool supporting the audit task. The first chapter of this article presents the applicable requirements arising from legal provisions and principles regarding the personal data protection in the employee recruitment process, as well as practical solutions in this regard. The next chapter focuses on verification principles recommended to ensure compliance with the law in the processing of personal data in the recruitment process. Subsequently, the most common risks and irregularities in this area are identified, along with guidelines to ensure compliance with legal regulations. The above study can serve in practice as a tool to help carry out the assurance task in question.

Legal provisions related to the processing of personal data of job candidates

The data controller, who is the employer, decides on the purposes and means of processing the personal data of job candidates. To ensure proper processing of job candidates’ personal data, compliance with the applicable principles and recruitment procedures of the Labour Code³ and the requirements of the GDPR in this regard must be ensured by the employer. The organizational and legal security of processed personal data undoubtedly affects the professionalism of the data controller and their perception by external clients, such as job candidates.

According to the viewpoint expressed in the literature, personal data is inalienable, which means that the entity processing it is merely its administrator. As rightly pointed out by A. Sobczyk, the employer – as the database admin-

¹ OJ L 119/1, 4.5.2016, hereinafter: GDPR.

² A. Szkuřłat, *Przetwarzanie danych osobowych przez pracodawców*, LEX/el. 2023.

³ Act of 26 June 1974 – Labour Code (consolidated text, Journal of Laws 2023, item 1465).

istrator – processes and utilizes knowledge about others' data, which does not become their property by the fact of processing.⁴ It should be emphasized that the recruitment procedures adopted in a given organization and the profile of the sought-after employee influence the recruitment process.⁵

Z. Góral and M. Kuba indicate that collecting information about job candidates should be qualified as processing personal data, understood as any operations performed on personal data, such as collection, recording, storage, adaptation, alteration, disclosure, and erasure.⁶

Article 5 of the GDPR lists principles regarding the processing of personal data.

K. Jaśkowski points out that from the perspective of processing personal data of job candidates, the key principles to consider are the principle of “lawfulness, fairness, and transparency” as regulated in Article 5(1)(a) of the GDPR, the principle of “purpose limitation”, which fundamentally requires collecting personal data only for specific, explicit, and legitimate purposes and not further processing them in a manner incompatible with those purposes (Article 5(1)(b) of the GDPR), and the principle of “data minimization”, which means agreeing to process only such data that are adequate, relevant, and limited to what is necessary for the purposes for which they are processed (Article 5(1)(c) of the GDPR).⁷

The implementation of the principle of “lawfulness” expressed in Article 5(1)(a) of the GDPR, further specified in Article 6 (1) of the GDPR which sets out the legal bases for processing data, occurs in cases where at least one of the following conditions is met:

- a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
- b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary to protect the vital interests of the data subject or of another natural person;
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

⁴ A. Sobczyk, *Przetwarzanie danych osobowych*, [in:] *Państwo zakładów pracy*, LEX/el. 2017.

⁵ Cf. I. Gocan, *Procedura zatrudniania krok po kroku*, LEX/el. 2024.

⁶ Z. Góral, M. Kuba, *Zakaz dyskryminacji kandydata do pracy a ochrona jego danych osobowych*, [in:] Z. Góral, M. Kuba, *Zakaz dyskryminacji w zatrudnieniu pracowniczym*, LEX/el. 2017.

⁷ K. Jaśkowski, [in:] E. Maniewska, K. Jaśkowski, *Kodeks pracy. Komentarz aktualizowany*, LEX/el. 2024, Article 22(1), Article 22(1)(a)), Article 22(1)(b)).

- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.⁸

In relation to the aforementioned legal basis for processing personal data as specified in Article 6(1)(c) of the GDPR, the personal data of job candidates may be processed based on the requirements indicated in Article 22¹ § of the Labour Code, which specifies that the employer requests from the person applying for employment to provide personal data including: first name(s) and surname, date of birth, contact details provided by such person, education, professional qualifications, and employment history. Here, certain personal data, such as parents' names or place of residence (correspondence address), as specified in the provision applicable until May 3, 2019, have been omitted, which is fully justified in the context of the data minimization principle arising from the GDPR. In § 2 of the aforementioned provision, the legislator specifies that the employer requests the provision of personal data referred to in § 1 points 4–6 when it is necessary for performing work of a specific type or in a specific position. Here, the importance of service pragmatics indicating the requirements necessary for the job, i.e. education or work experience, should be emphasised. In the literature, attention has been drawn to the fact that “the introduction of this limitation was justified by the fact that the legal norm does not exempt employers from the need to assess whether all the collected data are necessary for the purpose of hiring a specific individual. Not every employment relationship justifies the collection of information about education, professional qualifications, or previous employment history of the person applying for employment. According to the legislator, this regulation is intended to fully implement the principle of data minimization provided for in Article 5(1)(c) of the GDPR”⁹

Jaśkowski emphasizes that Article 22¹ of the Labour Code specifies three groups of personal data that an employer may request. The first group can be requested from the job candidate (§ 1), the second from the employee (§ 3), and the third (§ 4) from both the candidate and the employee. The employer cannot request the provision of other personal data.¹⁰

An employer, or typically a commission appointed by them, may reject a candidate's application if they have not met the formal requirements and have not

⁸ *Ibidem*.

⁹ D. Dörre-Kolasa, *Ochrona danych osobowych pracowników i kandydatów do pracy – zmiany od 4 maja 2019 r.*, LEX/el. 2018.

¹⁰ K. Jaśkowski, *op. cit.*

provided the required information specified in Article 22¹ § 1 of the Labour Code. In a situation where data other than those listed in the above article were to be transferred to employers, the legal basis for their processing would be the employee's consent. A. Szkuřat argues that the lack of consent or its withdrawal cannot be the basis for treating the job applicant unfavorably, nor can it result in any negative consequences for them, especially it cannot be a reason justifying refusal of employment.¹¹ A similar position is presented by I. Jaroszevska-Ignatowska and Z. Rosner-Laskorzyńska who emphasize that consent can be given in any form, although for evidentiary reasons it is worthwhile for it to be in writing (including by email), especially since the burden of proof that consent has been given lies with the data controller.¹²

Adopting such a solution in the case of processing ordinary data by the employer, and considering that candidates often provide surplus data in their application documents, such an interpretation would incline the employer to consistently obtain such consent from all candidates, which cannot be considered justified. In practice, there is a view that a candidate submitting their application in response to a specific job posting voluntarily provides personal data through their behavior in a free and unrestricted manner, which manifests as their conscious action indicating such consent. In practice, it is possible to encounter a situation where the employer assumes in advance in the advertisement a formal requirement for candidates to submit their consent to the processing of their personal data in connection with the application for a given job position, and then, in the absence of the candidate's declaration, rejects such an offer, which is an unfounded action, as the provisions of the labour law clearly indicate what data the employer may process. In the light of Article 4(11) of the GDPR, consent of the data subject should be voluntary, specific, informed, and unambiguous, given by a statement or clear affirmative action, allowing the processing of their personal data.

The candidate's consent to the processing of data for recruitment purposes can be withdrawn at any time. The prospective employer then loses the right to further process this data and should promptly delete it (the employer should inform the candidate of the right to withdraw consent at the time of obtaining their data). The lack of consent or its withdrawal cannot result in any negative consequences for the candidate, especially unfavorable treatment during the recruitment process.¹³

¹¹ A. Szkuřat, *op. cit.*

¹² I. Jaroszevska-Ignatowska, Z. Rosner-Laskorzyńska, *Przetwarzanie danych osobowych związanych z rodzicielstwem podczas procesu rekrutacji*, [in:] *Uprawnienia pracowników-rodziców*, LEX/el. 2021.

¹³ *Ibidem.*

Ordinary personal data, not falling within the catalog of obligatory data specified in labor law provisions, may be processed by the employer based on the candidate's consent, who submits their CV and cover letter to the employer.¹⁴

On the other hand, consent given at the request of the employer to collect and process their personal data violates the rights of the employee and their freedom to express their will. Recognizing the fact of the employee's consent as a circumstance legalizing the collection of data other than those specified in Article 22¹ of the Labour Code would circumvent this provision.¹⁵

This position has also been presented in case law, where it was clearly stated that an employer's instruction imposing on an employee the obligation to provide information (personal data) not listed in Article 22¹ §§ 1 and 2 of the Labour Code or in separate provisions (Article 22¹ § 4 of the Labour Code) is unlawful (Article 100 § 1 of the Labour Code), and therefore, refusal to comply with it cannot be the basis for termination of an employment contract under Article 52 § 1 point 1 of the Labour Code.¹⁶

An employer requests the provision of other personal data than those specified in Article 22¹ §§ 1 and 3 of the Labour Code when it is necessary to exercise a right or fulfill an obligation arising from a legal provision. M. Tomaszewska indicates that the legal basis determining the rules for processing personal data of job candidates and employed workers by employers are national regulations. Currently, it is Article 22¹ of the Labour Code and separate provisions.¹⁷ It is necessary to consider the official pragmatics specified in specific regulations. L. Florek and T. Zieliński emphasize that Article 51 of the Polish Constitution implies that these must be statutory provisions. This group also includes provisions that imply the obligation to obtain specific information about a person applying for employment or an employee, even if they do not explicitly state it. For example, when hiring for specific positions, appropriate health qualifications are required.¹⁸ The obligation to provide information in the recruitment process

¹⁴ M. Gumularz, P. Kozik, *Kontrole sektorowe 2019 – przetwarzanie danych w związku z rekrutacją*, LEX/el. 2019.

¹⁵ Judgment of the Supreme Court of October 17, 2018, II PK 178/17, No. 2562148; judgment of the Supreme Administrative Court of December 1, 2009, I OSK 249/09, ONSAiWSA 2011, no. 2, item 39.

¹⁶ Judgment of the Supreme Court of August 5, 2008, I PK 37/08, OSNP 2010, no. 1–2, item 4.

¹⁷ M. Tomaszewska, [in:] *Kodeks pracy. Komentarz*, vol. 1: Art. 1–93, red. K.W. Baran, LEX/el. 2022, Article 22(1).

¹⁸ L. Florek, T. Zieliński, [in:] D. Dzienisiuk, K. Gonera, G. Goździewicz, Ł. Pisarczyk, J. Skoczyński, J. Unterschütz, B. Wagner, P. Wojciechowski, L. Florek, T. Zieliński, *Kodeks pracy. Komentarz*, LEX/el. 2017, Article 22(1).

beyond those resulting from legal provisions cannot be established by the employer through internal regulations.¹⁹

In the literature, it is also pointed out that employee data (e.g., about family status, financial situation, or disability) are collected if their provision is necessary due to the employee's use of special rights provided for in labor law (Article 22¹ § 3 point 3 of the Labour Code) or if it is necessary to fulfill an employer's obligation imposed by a legal provision (Article 22¹ § 4 of the Labour Code).²⁰ It is emphasized that among the data requested during the recruitment process, there are none concerning pregnancy or family status, or parental plans.²¹

The above position was presented by the Supreme Court, which stated that the employer may request from the person applying for employment, and subsequently from the employee, to provide only those personal data that are clearly specified in the law (Article 22¹ §§ 1 and 3 of the Labour Code). The employer may request the provision of other personal data when it is necessary to exercise a right or fulfill an obligation arising from a legal provision (Article 22¹ § 4 of the Labour Code). Sensitive data, including data concerning health, are subject to special legal protection. There must be exceptional reasons for requiring an employee to disclose information about their health status, considering Article 9(1) and (2) of the GDPR.²² Article 22^{1b} § 1 of the Labour Code specifies that the consent of a person applying for employment or an employee may constitute the legal basis for the processing of personal data by the employer, referred to in Article 9(1) of the GDPR, only if the provision of such personal data is initiated by the person applying for employment or the employee.

Special category data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, sexual life, or sexual orientation of that person. Processing of such personal data may be allowed only by persons holding written authorisation to process issued by the employer. These individuals are required to keep this data confidential.²³ In this situation, apart from the requirement specified in Article 22^{1b} § 3 of the Labour Code, the content of Article 29 of the GDPR should also be cited, which specifies that any person acting on behalf of the data controller or data processor and having access to personal data processes them solely on the instructions of the controller unless required to do so by Union or

¹⁹ Z. Góral, M. Kuba, *op. cit.*

²⁰ M. Tomaszewska, *op. cit.*

²¹ I. Jaroszewska-Ignatowska, Z. Rosner-Laskorzyńska, *op. cit.*

²² Judgment of the Supreme Court of February 3, 2021, I PSKP 3/21, OSNP 2022, no. 1, item 2.

²³ I. Baranowska, *Zmiany w danych osobowych pracownika i kandydata do pracy od 4 maja 2019 r.*, LEX/el. 2019.

Member State law, which requirement applies to members of the recruitment committee commissioned by the employer.

In the context of job-related pragmatics indicated, among others, in Article 13a of the Act of November 21, 2008, on local government employees,²⁴ the entitlement related to the priority of employing disabled persons has been specified. According to paragraph 1 of the mentioned provision, during the recruitment process, the commission selects no more than five best candidates who meet the essential requirements and most of the additional requirements, presenting them to the unit manager for the purpose of employing the selected candidate. Paragraph 2 specifies that if the employment rate of disabled persons in the unit, as defined in the provisions on vocational and social rehabilitation and employment of disabled persons, in the month preceding the date of publication of the recruitment announcement, is lower than 6%, priority in employment for clerical positions, excluding managerial clerical positions, belongs to a disabled person, provided they are among the persons referred to in paragraph 1.

In the specified situation, undoubtedly, the situation defined in Article 9(2) (a) of the GDPR will apply, according to which the processing of special category data, as indicated in the above provision, will be permissible when the candidate submitting their application clearly consents to the processing of this personal data, thus through a specific statement confirmed by their handwritten signature.²⁵ Therefore, in this situation, the model statement added by the employer under the vacancy notice will be most appropriate.

The employer should process only such data that are necessary for the purpose of their collection, which is making a decision about employing a new employee. Here, it would be necessary to refer to the necessary requirements for the job specified in specific regulations. In other words, the employer cannot request from job candidates excessive data that are not necessary for conducting the recruitment process. Furthermore, the employer's request for job candidates to provide information beyond what is primarily provided for by labor law may violate both the provisions of the GDPR and labor law, raising, for example, the accusation of discrimination.²⁶

The Personal Data Protection Office (PDPO) also points out that according to Article 22¹ § 3 of the Labour Code, the provision of personal data to the employer is done in the form of a statement by the person to whom they relate, so it should be considered that the practice of additional verification of information obtained

²⁴ Consolidated text, Journal of Laws 2022, item 530.

²⁵ Cf. K. Hady-Głowiak, K. Kruczek, *Kontrola zarządcza a bezpieczeństwo informacji w procesie rekrutacji*, „Studia Kaliskie” 2022, vol. 10, p. 58.

²⁶ M. Gumularz, P. Kozik, *op. cit.*

from the candidate would violate the rights and freedoms of the individual. According to the PDPOs position, such a practice also does not find support in the provisions of the GDPR.²⁷ According to the PDPO, during the recruitment process, the source of information regarding the candidate's work history should be the candidate themselves.²⁸ It is unacceptable for a potential employer to obtain information about a job candidate from their previous employer without the candidate's consent. It is also worth remembering that submitting so-called references by a job candidate does not entitle the employer to contact the issuing entity to obtain additional information about the candidate.²⁹ It is also worth mentioning the attempt to verify information about the candidate on social media or other publicly available sources, which definitely leads to profiling the candidate without the required knowledge and consent, and may affect their negative assessment in the recruitment process. Bearing this in mind, precise indication by the employer in the recruitment announcement of the qualifications and documents necessary to confirm the essential requirements for the job position is crucial, and any attempt to unlawfully profile the candidate and process and obtain excess data without the required legal basis may expose the employer to both legal consequences and financial and reputational losses.

The profiling of job candidates for the purpose of selecting a suitable employee can therefore not take place without their knowledge, even if it were an ancillary activity not prejudging a specific decision towards the candidate. Furthermore, pursuant to Article 22 of the GDPR, if the decision to enter into or not to enter into an employment relationship were to be based solely on automated data processing, the candidate should also be informed of this fact in order to allow him/her to object to the profiling on the basis of Article 21(1) of the GDPR. Assessing candidates solely on the basis of profiling does not appear to be necessary for the conclusion of an employment contract. The purpose of selecting a suitable employee must not be carried out in a discriminatory manner. Automated attribution to a data subject of characteristics that he or she does not necessarily actually possess involves a high risk of unequal treatment, which can be minimised by human intervention in the process of assessing candidates and entrusting a human being to make the final decision on whether or not to enter into an employment relationship.³⁰

It should be noted that according to § 5 of the Regulation of the Minister of Family, Labour and Social Policy of 10 December 2018 on employee documen-

²⁷ Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, październik 2018, p. 16.

²⁸ *Ibidem*.

²⁹ M. Gumularz, P. Kozik, *op. cit.*

³⁰ J. Tlatlik, *Zakaz dyskryminacji na etapie nawiązywania stosunku pracy*, LEX/el. 2022.

tation,³¹ the employer keeps in the employee's personal files, kept in paper form, copies or extracts of documents submitted by the person applying for employment or the employee, certified by the employer or a person authorized by the employer as conforming to the submitted document.

In part A of the personal file, the employer is obliged to keep statements or documents specified in Article 22¹ § 1 and 4 of the Labour Code, consents to the processing of personal data other than those listed. The content of the introduced regulation indicates that the above-mentioned catalogue of data is closed, the only exception being the situation referred to in Article 22¹ § 4 of the Labour Code. If the recruitment process results in the employment relationship being established, it is these documents indicated above that the employer will be obliged, pursuant to § 3 item 1 of the above-mentioned regulation, to place in part A of the employee's personal file.³²

Another unwarranted action would be to require a candidate to produce documents in the form of a certificate from the National Criminal Register without the required legal basis, which is still practiced by some public entities today, or to keep copies of candidates' or employees' ID cards in their personal files. Thus, the scope of personal data in employee files must meet the criteria of the regulations in effect at the time of their acquisition and must not be redundant. An example here are the provisions of Article 4 of the Act of November 21, 2008, on the civil service,³³ which indicate that a person may be employed in the civil service who, among other things:

- 1) is a Polish citizen;
- 2) enjoys full public rights;
- 3) has not been sentenced by a final judgment for an intentional crime or an intentional fiscal crime;
- 4) has the qualifications required for the position;
- 5) enjoys a good reputation.

An analogous situation is presented in Article 6(3) of the Act on local government employees, where a local government employee employed on the basis of an employment contract for an official position may be a person who meets the following requirements:

- 1) is a Polish citizen;
- 2) has full legal capacity and enjoys full public rights;
- 3) has the professional qualifications required to perform work on a given position;

³¹ Consolidated text, Journal of Laws 2024, item 535.

³² J. Masłowski, *Akta osobowe pracowników – sposób prowadzenia*, LEX/el. 2021.

³³ Consolidated text, Journal of Laws 2024, item 409.

- 4) has at least secondary education or secondary vocational education;
- 5) has not been convicted by a final court sentence for a deliberate crime prosecuted by public indictment or a deliberate fiscal crime;
- 6) enjoys a good reputation.

In both cases, the aforementioned provisions do not provide grounds for the employer to require a certificate from the National Criminal Register from the candidate, however, to date such situations do occur.

According to the ruling of the Constitutional Tribunal, the protection of private life, guaranteed constitutionally in principle under Article 47, also encompasses informational autonomy (Article 51 of the Constitution), which means the right to independently decide on the disclosure of information concerning oneself, as well as the right to exercise control over such information if it is held by other entities.³⁴

Under Article 13 of the GDPR, the employer has an obligation to inform job candidates (employees) about the details regarding the processing of personal data obtained from them.³⁵ It is the Data Controller, therefore the employer, who is responsible for demonstrating compliance with the informational obligation towards job candidates. A good practice here is to include an information clause below the job posting, where the candidate responding to a specific advertisement can familiarize themselves with it.³⁶ The scope of information that should be included in the information clause should cover:

- 1) the identity of the Data Controller and contact details + possibly a representative;
- 2) contact details of the Data Protection Officer (if appointed);
- 3) purposes and legal basis for the processing of personal data;
- 4) legitimate interests;
- 5) information about recipients of personal data or categories of recipients;
- 6) information about the intention to transfer personal data to a third country or international organization;
- 7) data retention period;
- 8) information about the data subject's rights (access to data, data portability, objection, correction, deletion, etc.);
- 9) information about the right to withdraw consent;
- 10) information about the right to lodge a complaint with the supervisory authority;

³⁴ Judgment of the Constitutional Tribunal of November 20, 2002, K 41/02, OTK-A 2002, no. 6, item 83; judgment of the Constitutional Tribunal of February 19, 2002, U 3/01, OTK ZU 2002, no. 1, item 3.

³⁵ K. Jaśkowski, *op. cit.*

³⁶ K. Hady-Głowiak, K. Kruczek, *op. cit.*, p. 57.

- 11) whether providing data is a statutory or contractual requirement, or a condition of entering into a contract, and the consequences of not providing data;
- 12) information about automated decision-making, including profiling (principles of decision-making, significance, and consequences).

The correct implementation of the information obligation towards the job candidate is also related to the provision of precise and reliable information contained in the information obligation clause. It should be borne in mind here both the correct demonstration of the purposes and legal grounds for data processing, where often the controllers only show the legal grounds for processing arising from the provisions of Articles 6 and 9 of the GDPR without indicating the specific legal basis for the processing arising, for example, from the provisions of the labour law or professional pragmatics. Another error committed by controllers is the failure to indicate reliable information on the recipients of personal data or categories of recipients used by the controller, i.e. for example, entities providing technical and organisational services for remote recruitment.

The PDPO also emphasizes the issue of the data retention period for candidates. According to the institution, the data retention period for job candidates should be tailored to the principles of data processing and predetermined by the data controller.³⁷

At this point, attention should also be paid to the information regarding the data retention period included in the information clause and compare it with the information contained in the register of processing activities conducted in accordance with the requirement specified in Article 30 of the GDPR, where information is provided adequately as determined in the data controller's obligation to provide information. Furthermore, the PDPO emphasized that the employer should permanently delete the personal data of a candidate (e.g. by destruction or return) with whom they did not decide to enter into an employment contract immediately after the recruitment process, i.e. after signing an employment contract with the newly hired employee, unless other grounds justifying the data controller to process them have occurred.

The specific purposes of processing personal data should be clear, justified, and defined at the time of collection. Therefore, extending the data retention period contained in the application should be an exception to the rule of immediate deletion and should be particularly justified.³⁸

In the authors' opinion, the above position lacks justification, and retaining candidate data in such cases seems to be pointless, considering the documented

³⁷ Urząd Ochrony Danych Osobowych, *op. cit.*, p. 17.

³⁸ *Ibidem*.

course of the recruitment process based on a protocol prepared by the members of the commission appointed by the employer to conduct the recruitment. A good practice is to collectively and officially dispose of applications of candidates who were not directly accepted immediately after the recruitment process. This action will ensure compliance with the previously mentioned principles of data minimization and limitation of retention.

The Data Protection Office in its Guide for Employers pointed out that it is unacceptable to process data solely to protect against potential future and uncertain claims from the person to whom they relate.³⁹ This position also finds reflection in legal doctrine. Processing data solely to protect against potential future and uncertain claims from the person to whom they relate is impermissible. Otherwise, there may be doubt about how long personal data should be processed if that person decides not to bring a lawsuit against the employer. During the recruitment process, no contractual relationship arises between the job candidate and the employer.⁴⁰

In the absence of the candidate's consent, the employer cannot use their data obtained in a specific recruitment process for future recruitment purposes.⁴¹ Similar legal doubts arise when candidates submit their CVs outside the recruitment process, for example, electronically. In such a situation, the administrator should inform the candidate that the organization does not consider candidate documents outside the recruitment procedure and responds only to job offers submitted in response to a job vacancy announcement, and all received applications will be destroyed immediately upon receipt. It is good practice to inform about this procedure in the recruitment section of the respective unit or in response for received email.⁴²

Creating "blacklists" of job candidates is considered unacceptable. Moreover, there is no legal basis for exchanging information between employers about job candidates they do not want to hire. Additionally, it should be remembered that creating collections of negative data can lead to discrimination and making unfavorable decisions for individuals based on often unreliable, unjustifiably obtained information.⁴³

A cause of discrimination may also be the case of rejection of a candidate's offer for formal deficiencies, due to the candidate's failure to provide in his/her offer the employer's preferred contact details in the form of a telephone number or e-mail address, which is an action incompatible with the requirements of Article 22¹ of the Labour Code, due to the fact that other details were provided, e.g. a residential or correspondence address.

³⁹ *Ibidem*.

⁴⁰ M. Gumularz, P. Kozik, *op. cit.*

⁴¹ *Ibidem*.

⁴² K. Hady-Głowiak, K. Kruczek, *op. cit.*, p. 57.

⁴³ Urząd Ochrony Danych Osobowych, *op. cit.*, p. 19.

Practical aspects concerning the verification of compliance requirements for processing personal data in the recruitment process by the data controller and associated risks

In the literature, it has been pointed out that the most typical recruitment model is one in which the employer, as the data controller, independently obtains data from job candidates, for example, by posting an advertisement on their website under the “careers” section. A characteristic feature of such a model is the absence of using any “external” entities in the recruitment process and the coordination of the recruitment process by the employer’s personnel members. By the employer’s personnel members, we mean the entities referred to in Articles 29 and 32(4) of the GDPR, i.e. any natural person acting on behalf of the data controller, who has access to personal data and processes it solely on the controller’s instructions. It is also possible to use the services of external entities in the recruitment process – for example, by outsourcing the task of finding a candidate for the job or conducting technical activities related to recruitment (such as scheduling a meeting with the candidate, posting a job advertisement on a portal, providing IT tools for processing personal data in recruitment). Such an entity will most often act as a data processor, with whom, according to Article 28 of the GDPR, a data processing agreement must be concluded.⁴⁴

Using external entities in the recruitment process is also possible – for example, by commissioning such an entity to find a candidate for the employer or to perform technical tasks related to recruitment (such as scheduling a meeting with the candidate, posting a job advertisement on a portal, providing IT tools for processing personal data in recruitment). Such an entity will most often act as a data processor, and according to Article 28 of the GDPR, a data processing agreement should be concluded with them. It is important to distinguish between using a processor for recruitment purposes and a situation where the employer obtains personal data of candidates from a database collected by a recruitment agency (acting as the controller) for their own purposes, which involve collecting data of recruited individuals to provide them to potential employers who become – as recipients – controllers.⁴⁵

In this article, the model where the employer independently acquires data of job candidates, for example by posting a job advertisement on their website, was assessed.

To assess the legality of the recruitment process, as discussed in the previous chapter, practical documentation elements that should be considered for verifying

⁴⁴ M. Gumularz, P. Kozik, *op. cit.*

⁴⁵ *Ibidem.*

the compliance of processing personal data of job candidates in the recruitment process, along with practical guidelines, are presented below in a tabular format.

Table 1. Example documentation for conducting an assessment of the compliance of processing personal data of job candidates in the recruitment process along with practical guidelines

The proposed documentation for assessing the compliance of processing personal data of job candidates in the recruitment process	Subject of verification
The employee recruitment procedure	Verification of legal grounds arising from labor law provisions as well as additional administrative practices defining the principles of conducting the recruitment process. Attention should be paid to the procedures for appointing the Employee Recruitment Committee and the manner in which tasks are carried out in accordance with principles of legality, data storage limitation, and minimization. The recruitment procedures at various stages of the hiring process should be reviewed to ensure that there is no candidate profiling or collection of surplus data* (such as through recruitment techniques like attempting to verify information about the candidate from their previous employer or on social media and other publicly available sources, or asking surplus questions not compliant with labor law requirements during the interview). Additionally, scrutiny should be given to any discrimination against employees due to failure to provide preferred contact information requested by the employer, or the manner in which questions indicated in the assessment protocols by the committee are asked. It is worth noting how the committee informs candidates about meeting formal requirements. It should be verified whether in the vacancy notice the employer does not require additional declarations from candidates in the form of consent to the processing of their personal data (in addition to consent to the processing of special category personal data) and, in the absence of such consent, whether offers have not been unjustifiably rejected on this ground
The job advertisement, including the personal questionnaire for job candidates	Verification of mandatory and additional requirements for compliance with Article 22 ¹ § 1 of the Labor Code and administrative practices, as well as the principle of data minimization. It is also necessary to assess the established procedures for handling offers submitted by candidates outside the recruitment procedure

The proposed documentation for assessing the compliance of processing personal data of job candidates in the recruitment process	Subject of verification
The manner in which the employer fulfills the information obligation in the recruitment process (e.g. in the selected recruitment announcement for verification) and its correlation with the employee recruitment process specified in the processing activities register	Verification of how the obligation to provide information to job candidates has been fulfilled and documented, such as in the job advertisement. Attention should be paid to elements such as the legal basis for data processing, including the legal grounds for processing, recipients of personal data, and the retention period for personal data. It is necessary to check how the employer proceeds if there are special category data in the advertisement and whether the advertisement for recruitment requires a relevant declaration in this regard in accordance with Article 9(2)(a) of the GDPR confirmed by a handwritten signature, in line with administrative practices resulting, for example, from the Act on Local Government Employees
Record of individuals authorized to process personal data and authorizations for processing personal data for members of the team/committee responsible for recruitment of employees associated with the selected employee recruitment process	Verification of whether the members of the commission had the appropriate authorizations to process data in the recruitment process, including the validity period and adequate notation in the authorization register. Additionally, it should be verified whether the members of the commission signed relevant confidentiality and impartiality statements and examine whether there are, in fact, any grounds for violating these provisions
Disposing of applications from candidates not accepted for employment after the recruitment process has been completed	It should be verified whether the data of candidates who were not accepted are protocolled properly after the recruitment process, in accordance with the information specified in the obligation to inform. It is also worth noting whether the employer does not store data excessively, justifying it by the possibility of future claims, which is unacceptable. It is also worth reviewing the extent of personal data in the employee file to ensure that it meets the criteria of the legislation in force at the time it was obtained from the candidate in line with the applicable legislation, so that it is not redundant

* See K. Hady-Głowiak, K. Kruczek, *Kontrola zarządcza a bezpieczeństwo informacji w procesie rekrutacji*, „Studia Kaliskie” 2022, vol. 10, p. 58.

Source: Authors' own study.

Among the risks that may arise in connection with verifying individual elements related to the processing of employees' personal data in the recruitment process, considering the irregularities presented in the first chapter of this article, the following should be mentioned in particular:

- non-compliance with or lack of applicable rules and procedures or their inconsistency with applicable legal regulations;

- unauthorized access to personal data;
- processing of personal data without clear legal basis or in violation of the principle of data minimization and limitation of storage.

Conclusion

The organizational and legal security of processed personal data undoubtedly affects the professionalism of the administrator and their perception by external clients, who are job candidates.

Individuals authorized to process data in the recruitment process are required to keep it confidential. Each member of the recruitment committee must receive authorization from the administrator to process the personal data of job candidates before participating in the recruitment process.⁴⁶ Additionally, each member of the committee, along with the authorization to process personal data received, should sign a confidentiality and impartiality statement to ensure full transparency in the recruitment process.

To ensure full transparency and impartiality in the recruitment process, the assessment conducted by the committee should be entirely objective, and the committee itself should be a specialized advisory body composed of independent external advisors. Only then can we talk about the competitiveness of the recruitment process.⁴⁷ Therefore, in the first chapter of this article, common irregularities related to attempts to profile candidates through additional verification in publicly available sources or with previous employers were pointed out, which can negatively affect the assessment of the candidate.

Discrimination may also occur when a candidate's offer is rejected due to formal deficiencies, such as not providing preferred contact details in the offer, such as a phone number or email address, because other information, such as home address or correspondence address, was provided. In other words, the employer cannot demand excessive data from the candidate that is not necessary for the recruitment process. Moreover, the employer's request for information beyond what is primarily provided for by labor law provisions may violate both the provisions of the GDPR and labor law, giving rise to accusations of discrimination.

The processing of data during the recruitment process will be lawful only upon presenting a legal basis, which will include: a legal obligation (arising from labor law provisions or other national or EU regulations), e.g. Article 22¹ of the

⁴⁶ K. Hady-Głowiak, K. Kruczek, *op. cit.*, p. 62.

⁴⁷ S. Głowiak, *Aspekty administracyjnoprawne w zakresie prawidłowości procesu naboru pracowników samorządowych w świetle orzecznictwa sądownoadministracyjnego*, LEX/el. 2011.

Labor Code, the employee's consent, the legitimate interest of the employer, and public interest.⁴⁸

In the case of a candidate providing excess data in response to a specific job advertisement by behaving freely and unrestrictedly, the candidate voluntarily discloses personal data, which manifests as their conscious action indicating such consent in accordance with the requirements of Article 4(11) of the GDPR. In light of the above, it should be assumed that requesting additional statements from the candidate will be doubtful.

According to Article 22^{1b} § 1 of the Labor Code, the consent of a job applicant or an employee may constitute the basis for the employer to process personal data referred to in Article 9(1) of the GDPR, only if the provision of such personal data is initiated by the job applicant or the employee, confirmed by a statement with a handwritten signature. Such a situation may arise when a candidate wishes to avail themselves of priority in employment as specified in official business practices.

Precisely specifying in the job advertisement the qualifications and documents necessary to confirm the requirements for the job position is crucial, and any attempt to unlawfully profile the candidate, as well as processing and acquiring excess data without the required legal basis, may expose the employer to legal consequences, as well as financial and reputational losses.

Verification of how the obligation to inform candidates for a job was fulfilled, for example, in the job announcement, needs to be conducted. Attention should be paid to elements such as the legal basis for processing data, including legal grounds for processing, recipients of personal data, and the retention period for personal data. It should be verified whether the data of candidates who were not accepted are protocolled after the recruitment process in accordance with the information specified in the obligation to inform. It is also important to check whether the employer does not store data excessively, justifying it by potential future claims, which is impermissible.

Another crucial aspect is the retention period of candidates' personal data, which should be adjusted to the principles of data processing and predetermined by the data controller. Key will be the answer to whether rules for handling offers from candidates submitted outside the recruitment procedure have been established.

Lastly, it is worth mentioning the standpoint cited in the literature that, to ensure clear and transparent recruitment procedures, it is advisable for an inspector to participate in creating recruitment rules, followed by their verification through audits. Transparency in this process will positively impact the organiza-

⁴⁸ M. Mędrala, *RODO – bezpieczeństwo danych osobowych w dziale kadr*, LEX/el. 2018.

tion's image and refute allegations of nepotism. It is also important to emphasize the role of auditors in the process of creating these rules.⁴⁹

A crucial element of implementing GDPR is the awareness among staff and employees of various legal solutions. To achieve this, it is necessary to train management and HR department employees and implement an internal control system, which can also be part of the data security and protection policy.⁵⁰

References

- Baranowska I., *Zmiany w danych osobowych pracownika i kandydata do pracy od 4 maja 2019 r.*, LEX/el. 2019.
- Dörre-Kolasa D., *Ochrona danych osobowych pracowników i kandydatów do pracy – zmiany od 4 maja 2019 r.*, LEX/el. 2018.
- Florek L., Zieliński T., [in:] D. Dzieńsiuk, K. Gonera, G. Goździewicz, Ł. Pisarczyk, J. Skoczyński, J. Unterschütz, B. Wagner, P. Wojciechowski, L. Florek, T. Zieliński, *Kodeks pracy. Komentarz*, Warszawa 2017.
- Głowiak S., *Aspekty administracyjnoprawne w zakresie prawidłowości procesu naboru pracowników samorządowych w świetle orzecznictwa sądownoadministracyjnego*, LEX/el. 2011.
- Gocan I., *Procedura zatrudniania krok po kroku*, LEX/el. 2024.
- Góral Z., Kuba M., *Zakaz dyskryminacji kandydata do pracy a ochrona jego danych osobowych*, [in:] Z. Góral, M. Kuba, *Zakaz dyskryminacji w zatrudnieniu pracowniczym*, Warszawa 2017.
- Gumularz M., Kozik P., *Kontrole sektorowe 2019 – przetwarzanie danych w związku z rekrutacją*, LEX/el. 2019.
- Hady-Głowiak K., Kruczek K., *Kontrola zarządcza a bezpieczeństwo informacji w procesie rekrutacji*, „Studia Kaliskie” 2022, vol. 10.
- Jaśkowski K., [in:] E. Maniewska, K. Jaśkowski, *Kodeks pracy. Komentarz aktualizowany*, LEX/el. 2024.
- Jaroszewska-Ignatowska I., Rosner-Laskorzyńska Z., *Przetwarzanie danych osobowych związanych z rodzicielstwem podczas procesu rekrutacji*, [in:] I. Jaroszewska-Ignatowska, Z. Rosner-Laskorzyńska, *Uprawnienia pracowników-rodziców*, LEX/el. 2021.
- Masłowski J., *Akta osobowe pracowników – sposób prowadzenia*, LEX/el. 2021.
- Mędrala M., *RODO – bezpieczeństwo danych osobowych w dziale kadr*, LEX/el. 2018.
- Sobczyk A., *Przetwarzanie danych osobowych*, [in:] *Państwo zakładów pracy*, Warszawa 2017.
- Szkuřat A., *Przetwarzanie danych osobowych przez pracodawców*, LEX/el. 2023.
- Tłatlik J., *Zakaz dyskryminacji na etapie nawiązywania stosunku pracy*, LEX/el. 2022.
- Tomaszewska M., [in:] *Kodeks pracy. Komentarz*, vol. 1: Art. 1–93, red. K.W. Baran, Warszawa 2022.
- Urząd Ochrony Danych Osobowych, *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców*, październik 2018.

⁴⁹ K. Hady-Głowiak, K. Kruczek, *op. cit.*, p. 62.

⁵⁰ M. Mędrala, *op. cit.*

Abstract: The subject of this article is to identify good practices, occurring risks and irregularities in the processing of personal data of job candidates as part of the employee recruitment process and to develop principles for verifying the correctness of the functioning of this process as a tool supporting the audit task. The recruitment process and the associated staff turnover is one of the key areas where the employer should ensure the organizational and legal security of the processed personal data, which undeniably affects its professionalism and the perception of external customers, such as job candidates. The uniformity of the legality of this process is influenced by both national labor laws and EU regulations. The key principles to ensure the compliance of processed data with the requirements of labor laws in the recruitment process are the principle of data minimization and storage limitation, as well as the processing of personal data of job candidates by persons only authorized by the employer, who have committed themselves to the principles of confidentiality and impartiality. The above is also related to the implementation of the controller's information obligations to job candidates and their correlation with the actual processing of personal data by the controller and its authorized personnel.

Keywords: labor law; employee recruitment; data protection

Abstrakt: Przedmiotem artykułu jest wskazanie dobrych praktyk, występujących ryzyk i nieprawidłowości w zakresie przetwarzania danych osobowych kandydatów do pracy w ramach procesu naboru pracowników oraz wypracowanie zasad weryfikacji oceny prawidłowości funkcjonowania tego procesu jako narzędzia wspomagającego realizację zadania audytowego. Proces rekrutacji i związana z tym fluktuacja kadr są jednym z kluczowych obszarów, gdzie pracodawca powinien zapewnić bezpieczeństwo organizacyjne i prawne przetwarzanych danych osobowych, co bezsprzecznie wpływa na jego profesjonalizm oraz postrzeganie przez klientów zewnętrznych, jakimi są kandydaci do pracy. Na ujednolicenie legalności tego procesu wpływ mają zarówno krajowe przepisy prawa pracy, jak i przepisy unijne. Do kluczowych zasad mających na celu zapewnienie zgodności przetwarzanych danych z wymogami przepisów prawa pracy w procesie rekrutacji należy zaliczyć zasadę minimalizacji danych i ograniczenia przechowywania oraz przetwarzanie danych osobowych kandydatów do pracy przez osoby wyłącznie upoważnione przez pracodawcę, które zobowiązały się do przestrzegania zasad poufności i bezstronności. Wiąże się to również z prawidłową realizacją obowiązków informacyjnych administratora wobec kandydatów do pracy oraz ich korelacją z rzeczywistym sposobem przetwarzania danych osobowych przez administratora i upoważniony przez niego personel.

Słowa kluczowe: prawo pracy; rekrutacja pracowników; ochrona danych osobowych