Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

Articles

Studia Iuridica Lublinensia vol. XXX, 4, 2021
DOI: 10.17951/sil.2021.30.4.593-603

Sylwia Zaborska
Maria Curie-Skłodowska University in Lublin, Poland
ORCID: 0000-0002-9811-9995
sylwia.zaborska@umcs.pl

Selected Legal Aspects of Processing Employee Biometric Data

Wybrane aspekty prawne dotyczące przetwarzania danych biometrycznych pracowników

ABSTRACT

Given the growing popularity of biometrics, doubts about the conditions for biometric data processing can be noticed in practice. These inaccuracies take place in various areas of law, including labour law. This article provides a theoretical discussion on the processing of special categories of data. It aims to point to the need for appropriate legal regulations to ensure the security of the processing of biometric data of employees and candidate employees. The article starts with clarifying the concept of biometric data and discusses the practical aspects of the use of biometric tools. Further on, the author analyses the legal regulations concerning the processing of biometric data in the relations between the employer as the personal data controller and the employee as the data subject. As a result of the studies carried out, a position was presented which indicates that the employer who processes biometric data of employees and candidates for employment should always find out whether he has legal justification to process the data in question. This article is one of the few studies on the processing of biometric data in Polish literature on the subject. The main purpose hereof is to present situations under the current legislation, in which the employer can process biometric data of its employees. The article is a form of universal presentation of the problem and may be of interest especially to legal practitioners.

Keywords: biometrics; biometric data; labour law; biometric tools

CORRESPONDENCE ADDRESS: Sylwia Zaborska, MA in Law, Assistant Lecturer, Maria Curie-Skłodowska University (Lublin), Faculty of Law and Administration, Institute of Law, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

INTRODUCTION

Verification and identification of persons using cards, codes or PINs is becoming less and less popular. This is mainly due to the development of new technologies using biometric techniques. These techniques allow fast and convenient identity confirmation without the need to remember complex passwords. The growth in importance of biometric systems should be attributed to the fact that biometric features are universal (every person has them), unique (they are different in every person) and are permanent because they generally do not change.[1] Furthermore, when using biometrics, one is not afraid about forgetting the code or losing the keys, thus posing a risk of providing confidential information to third parties. In practice, biometric tools are mainly used as access control measures, guaranteeing a high degree of security.[2] Also in the area of the employer-employee relationship, it should be noted that the use of biometrics is becoming more and more common. This is particularly related to recording the employee's working time and securing the premises against unauthorised access.[3] In view of the growing trend in the use of biometric solutions, the need to regulate the processing of employee biometric data has become unavoidable. Employers, each time they use personal data of their employees, should be aware of the legal consequences resulting from the unlawful processing of personal data.

The purpose of this article is to draw attention to the role played by the employer in processing biometric data of employees and candidate employees. An analysis of legal regulations on the processing of biometric data in relations between the employer as the personal data controller and the employee as the subject whose data are processed leads to the conclusion that the employer should each time determine whether he meets the legal prerequisite to make the processing of the data in question lawful.

CONCEPT OF BIOMETRIC DATA

In the terminology of IT sciences, biometrics is defined as a technology for automatic identity recognition based on human biological traits. The literature on the subject distinguishes between static characteristics, such as appearance of fingerprint pattern, and dynamic characteristics, closely related to human behaviour

[1] Article 29 – Data Protection Working Party, Working document in biometrics, Adopted on 1 August 2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf [access: 10.08.2021], p. 3.

[2] D. Gutowska, *Techniki identyfikacji osób z wykorzystaniem indywidualnych cech biometrycznych*, "Zeszyty Naukowe Wydziału Elektroniki i Automatyki Politechniki Gdańskiej" 2004, no. 20, p. 69.

[3] M. Tomaszewska-Michalak, *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Warszawa 2015, p. 110.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

such as the dynamics of walking or the way of making a signature.[4] Unique features of the body, organism or behaviour of each person are referred to as biometric characteristics.[5] With the growing use of biometric solutions and techniques, the need for appropriate legal regulations has also arisen.[6] In the legal situation defined by the provisions of Directive 95/46/EC,[7] the determination of the conditions of admissibility and lawfulness of the processing of biometric data caused a number of uncertainties. This was mainly due to the lack of a legal definition of biometric data.[8] Directive 95/46/EC did not directly address the issue in question. The main source of knowledge concerning the relationship between the law and biometrics were the opinions developed by the Article 29 Data Protection Working Party.[9] It is only under 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[10] that biometric data has been recognised as special categories of data,[11] similarly to personal data revealing political opinions, data concerning health or data concerning sexual orientation.[12] These types of data are thus more protected than normal data. The higher standard of protection results, first of all, from the specific character of the processed information. According to the legal definition provided for in Article 4 (14) GDPR, "biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. Specific technical processing should be understood as the use of methods and means for the analysis of biometric characteristics to identify an individual, such as retinal scanning. The

[4] W. Gutfeter, A. Pacut, *Człowiek w systemie biometrycznym*, [in:] *Dokumenty a prawo*, eds. M. Tomaszewska-Michalak, T. Tomaszewski, Warszawa 2015, p. 79.

[5] A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018, p. 118.

[6] D. Jaroszewska-Choraś, *Biometria. Aspekty prawne*, Gdańsk 2016, p. 17.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, pp. 31–50), hereinafter: Directive 95/46/EC.

[8] Biometric data under the legislation previously in force was neither classified as sensitive data nor as ordinary data. See A. Krasuski, *op. cit.*, p. 118.

[9] For more detail on the Working Party, see the website of the Polish Personal Data Protection Office, https://uodo.gov.pl/57 [access: 07.02.2020].

[10] OJ L 119, 4.05.2016, pp. 1–88, hereinafter: GDPR.

[11] The division of data into ordinary and sensitive data plays an important role in terms of the duties of personal data controllers, in particular in the analysis of the data risk assessment and the related security of processing, the recording of activities and the mandatory appointment of a personal data protection officer (D. Lubasz, *Dane zwykłe i szczególne kategorie danych*, [in:] *RODO w e-commerce*, ed. D. Lubasz, Warszawa 2018).

[12] The catalogue of particularly protected data is of a closed character and has been provided in Article 9 (1) GDPR.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

processing of biometric data is, as a rule, prohibited. However, this prohibition is not absolute, as certain prerequisites have been identified which allow the lawful processing of special categories of data. Apart from the circumstances explicitly mentioned in Article 9 (2) GDPR, the EU lawmakers have also given Member States the right to introduce additional exceptions to the prohibition on processing genetic, biometric or health-related data (Article 9 (4) GDPR).

BIOMETRIC DATA PROCESSING AS REGULATED IN THE LABOUR CODE

As a result of the amendment of the Labour Code of 4 May 2019 by the Act of 21 February 2019 amending certain other acts in order to ensure the application of 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,[13] the Polish legislature has adapted the Polish labour law to the wording of EU legislation. Article 22^{1b} was added to the Labour Code[14] to address directly the processing of sensitive data by the employer. According to the wording of this provision, the consent of a job candidate or an employee may constitute the basis for the processing by the employer of personal data referred to in Article 9 (1) GDPR, only if the transfer of such personal data takes place on the initiative of the candidate or the employee. On the other hand, § 2 of Article 22^{1b} states that the processing of employee's biometric data is also permissible if the provision of such data is necessary for the control of access to particularly important information the disclosure of which may be detrimental to the employer, or for access to premises requiring special protection.[15]

Consequently, the Labour Code sets out two conditions which entitle the employer to lawfully process biometric data. The first is consent, which should be voluntary, unambiguous, informed and prior. The second is the necessity of processing for the control of access to particularly important information and premises.

When referring to the consent-based processing of special category data, including biometric data, it should be borne in mind that in this case, the condition for validity of the consent is providing it at the initiative of the job candidate or

[13] Journal of Laws 2019, item 730.

[14] Act of 26 June 1974 – Labour Code (consolidated text, Journal of Laws 2020, item 1320).

[15] It should be noted that the regulation contained in Article 22^{1b} of the Labour Code is a regulation of a special nature as compared to the norm contained in Article 22^{1a} of the Labour Code, which refers to the employer's processing of employee's personal data only based on the employee's or candidate's consent.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

employee. Unlike in the case of transferring ordinary data, which may be collected at the initiative of the employer, employee and job candidate.[16] The subjective limitation of the group of individuals authorized to provide consent is associated with the threat to personal data protection resulting from the imbalance of power between the parties to the employment relationship. Considering the correlation taking place between the employer and the employee, there may be a fear that the employee, afraid of negative consequences, will not be able to refuse the employer requiring consent to the processing of their data.[17] The limitation of the possibility to process employee's or job candidate's sensitive data on the basis of consent only to the data provided to the employer at the initiative of the employee or job candidate is a manifestation of an increased degree of protection of sensual data.[18] This leads to the conclusion that the purpose of the regulation is also to prevent the employer from suggesting the employee to provide particularly protected data. In fact, the employer may not even initiate a process that would involve the processing of particularly protected data, even if employees support and accept the process in question.[19]

The employer's economic advantage over the employee and the situation on the labour market may result in the consent being ostensible. In this respect, particularly relevant in the field of labour law is Article 7 (4) GDPR, according to which, when assessing whether consent is freely given, utmost account shall be taken of whether, i.a., the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. In addition, explicit consent is required for sensitive data. The qualified form of consent is justified primarily by the protection of privacy. The consent should have the form of clear action, e.g. by a statement of the employee. A confirmatory action involving only a permission for the processing of personal data will not have the character of express consent. It should also be noted that the position of the Polish Supreme Administrative Court, which in its judgement of 2009 clearly stated that the employee's written consent to the collection and processing of his personal data, expressed at the employer's request, infringes the employee's rights and the freedom to express his will. This view is supported by the employee's dependence on the employer. The unbalance in the relationship between the employer and the employee makes questionable the voluntary nature of the consent to the collection and processing of personal (biometric) data.[20]

---

[16] M. Nałęcz, [in:] *Kodeks pracy. Komentarz*, ed. W. Muszalski, Warszawa 2019, p. 58.

[17] *Ibidem*.

[18] M. Kuba, [in:] *Kodeks pracy. Komentarz*, ed. K.W. Baran, vol. 1, Warszawa 2020, p. 240.

[19] J. Jarguz, [in:] *Kodeks pracy. Komentarz*, ed. A. Sobczyk, Warszawa 2020, p. 127.

[20] Judgement of the Supreme Administrative Court of 1 December 2009, I OSK 249/09, Legalis no. 332309.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

It is therefore obvious that the norm contained in Article 22^{1b} § 1 of the Labour Code constitutes an additional restriction on the processing of biometric data under labour law. Apart from the qualified form of consent under Article 9 (2) (a) GDPR, it is also necessary to determine on whose initiative the transfer of sensitive data takes place. Only when these two conditions are met cumulatively, the data controller – the employer – is entitled to lawfully process sensitive data. It also needs to be stressed that the granting of personal data consent is a reversible decision which is within control of the data subject. By making an appropriate reference to Article 22^{1a} § 2 of the Labour Code, the legislature clearly stated that the absence or withdrawal of consent may not give rise to unfavourable treatment for the employee, nor can it have any negative consequences for the employee, in particular, it may not constitute a reason for termination of the contract with or without notice by the employer. This regulation allows the principle of voluntary consent and the right of withdrawal to be implemented.[21] The possibility of withdrawing the consent gives the data subject a certain scope of freedom and control.

Another situation that entitles the employer to lawfully process biometric data is related to the circumstance in which such data must be provided for the purposes of the control of access to particularly important information, the disclosure of which could expose the employer to a loss, or the control of access to premises requiring special protection. A necessary criterion for the application of this exception is the actual existence of separate places within the workplace where protected essential information is stored.[22] Verification of access to such places using biometric methods does not require the employer to obtain additional consent from the employees for processing their personal data.[23] In such a situation, a precondition for the processing of personal data will be the legitimate interest of the employer, assessed together with the necessity of the access control measures.[24] As underlined in the opinion of the Article 29 Working Party, this type of interest is only legitimate if the data controller – the employer – can prove that its interest is objectively superior to the data subject's right not to be registered in the biometric system.[25] As far as the

[21] M. Nałęcz, *op. cit.*, p. 57.

[22] There are proposals in the literature on the subject, according to which the legislature should extend the necessity of access protection, apart from premises, also to relevant devices or other items that require particular protection. See M. Kuba, *Administrator Danych Biometrycznych – wybrane zagadnienia*, [in:] *Administrator i inspektor ochrony danych osobowych*, eds. M.A. Mielczarek, T. Wyka, Warszawa 2019, p. 101.

[23] U. Torbus, [in:] *RODO. Ochrona danych osobowych w zatrudnieniu ze wzorami*, ed. M. Mędrala, Warszawa 2018, p. 102.

[24] M. Nałęcz, *op. cit.*, p. 57.

[25] In the opinion of the Article 29 Working Party, it is legitimate to use biometric technology, e.g., if a high level of safety and strict control of access to a research laboratory for the study of dangerous viruses are necessary. Access secured by doors that open only after a successful fingerprint and iris scan verification is justified by the need to make sure that only the persons familiar with the

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

necessity of access control measures is concerned, E. Suknarowska-Drzewiecka argues that, in view of the value of personal data protection, this concept may not be assessed according to the employer's subjective conviction.[26] Also M. Nałęcz notes that this necessity should be assessed in relation to the value of personal data protection.[27] This leads to the conclusion that the use of biometric control measures by the employer should be preceded by a detailed analysis of two conditions: the employer's interest and the necessity of the use of access control measures.

The legislature has also introduced a subjective restriction as regards persons authorized to process biometric data and other special data specified in § 1 of Article 22^{1b} of the Labour Code. Only those with a written authorization to process such data issued by the employer may be allowed to process such data. Due to the need for strict protection of biometric data, it is emphasized in the literature on the subject that a written authorization should be granted in a separate document describing the specific data to which the employee will have access and to what extent the data will be processed.[28] Individuals admitted to the processing of such data shall be bound by the obligation of confidentiality (Article 22^{1b} § 3 of the Labour Code). However, a certain legislative inaccuracy should be pointed out. The legislature referred the solution discussed above only to sensitive data processed under consent of the data subject. It would be reasonable to extend the additional security in the form of the requirement to grant the relevant authorization also in respect of the biometric data referred to in Article 22^{1b} § 2 of the Labour Code.

EMPLOYEE BIOMETRIC DATA PROCESSING FOR WORKING TIME MANAGEMENT

Due to the ease and convenience of using biometric technology, employers have been more and more willing to think about the possibility of using biometrics for working time control. This is so because the possibility to record working time using a fingerprint reader instead of signing attendance lists or reading magnetic cards would be a significant improvement.

However, the current rules do not provide for the legal possibility of processing employees' biometric data to control their working time.[29] The case law according to which such a form of control under the new legislation is disproportionate to

specific risks and trained can experiment with these dangerous materials. See Article 29 Working Party, Opinion 3/2012 on developments in biometric technologies WP 193, p. 13.

[26] E. Suknarowska-Drzewiecka, [in:] *Kodeks pracy. Komentarz 2020*, ed. K. Walczak, Legalis.

[27] M. Nałęcz, *op. cit.*, p. 58.

[28] *Ibidem*.

[29] D. Jarmużek, [in:] *RODO. Ochrona danych osobowych w stosunkach pracy*, eds. E. Jagiełło-Jaroszewska, D. Jarmużek, P. Zawadzka-Filipczyk, Warszawa 2018, pp. 92–93.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

the intended purpose of processing these data remains valid.[30] Noteworthy is the position of the Inspector General for Personal Data Protection, in whose opinion recording the entry and exit by the personnel cannot be made using a fingerprint scanning system, as this leads to a violation of the principle of adequacy of data processing, as these objectives may be achieved by other means or by other techniques not directly linked to the processing of biometric data.[31]

In the decision of 18 February 2020, the President of the Personal Data Protection Office confirmed that the processing of employee biometric data by the employer cannot serve the purpose of working time records.[32] He pointed out that, by their very nature, this type of data could only be processed in exceptional circumstances. The employer has other tools in place to record employee working time effectively, without the need to use modern biometric data technologies. At the same time, the President of the Personal Data Protection Office pointed out that the employer, using the biometric data of an employee to record his or her working time would violate the rules set out in the GDPR. The employer would then act contrary to the principles of legality, limitation of purpose and data minimisation, since it would not be able to prove on what legal basis he processes employee biometric data for the sole purpose of recording working time.[33] Thus, under the current legislation, employers cannot process the biometric data of their employees to verify their presence at work. Attendance lists or individual identifiers must continue to be used for this purpose.

CONCLUSIONS

The processing of biometric data, due to its specific nature, carries a high risk of infringement of the rights and freedoms of data subjects. The infringement may take place in particular within the relationship between the employer and the employee. So there was a need to ensure an adequate level of security of biometric data of employees and job candidates.

The employer, as the controller of personal data of employees and job candidates, should only process biometric data in each case if there is a legal basis for doing so. If the basis for the processing is a "consent", the consent should be specific, informed, clear and voluntary and the withdrawal of consent should not have any negative

[30] Judgement of the Supreme Administrative Court of 1 December 2009, I OSK 249/09, Legalis no. 332309.

[31] Decision of the Inspector General for Personal Data Protection of 23 September 2010, DIS/DEC-1133/37986/10.

[32] Decision of the President of the Personal Data Protection Office of 18 February 2020, ZSZZS.440.768.2018.

[33] *Ibidem*.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

consequences for the employee. But it also must be stressed that the employer, when processing biometric data, must adhere to the basic principles set out in the GDPR, which include, among others, the principle of adequacy and the principle of minimisation. According to the principle of adequacy, the controller is obliged to limit the scope of data processing only to the data which are necessary to fulfil the controller's own legitimate objective. Therefore, if the controller can achieve the same result by processing less sensitive data than biometric data, the controller should choose this method. At the same time, the data to be collected by the employer must be limited to the minimum necessary to achieve the objective assumed.[34] Employers are therefore required to maintain a balance between their own interests and the personal interests of their employees, especially the right to privacy.

REFERENCES

Literature

Czarnowski A., [in:] *RODO. Przewodnik ze wzorami*, ed. M. Gawroński, Warszawa 2018.

Gutfeter W., Pacut A., *Człowiek w systemie biometrycznym*, [in:] *Dokumenty a prawo*, eds. M. Tomaszewska-Michalak, T. Tomaszewski, Warszawa 2015.

Gutowska D., *Techniki identyfikacji osób z wykorzystaniem indywidualnych cech biometrycznych*, "Zeszyty Naukowe Wydziału Elektroniki i Automatyki Politechniki Gdańskiej" 2004, no. 20.

Jarguz J., [in:] *Kodeks pracy. Komentarz*, ed. A. Sobczyk, Warszawa 2020.

Jarmużek D., [in:] *RODO. Ochrona danych osobowych w stosunkach pracy*, eds. E. Jagiełło-Jaroszewska, D. Jarmużek, P. Zawadzka-Filipczyk, Warszawa 2018.

Jaroszewska-Choraś D., *Biometria. Aspekty prawne*, Gdańsk 2016.

Krasuski A., *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018.

Kuba M., [in:] *Kodeks pracy. Komentarz*, ed. K.W. Baran, vol. 1, Warszawa 2020.

Kuba M., *Administrator Danych Biometrycznych – wybrane zagadnienia*, [in:] *Administrator i inspektor ochrony danych osobowych*, eds. M.A. Mielczarek, T. Wyka, Warszawa 2019.

Lubasz D., *Dane zwykłe i szczególne kategorie danych*, [in:] *RODO w e-commerce*, ed. D. Lubasz, Warszawa 2018.

Nałęcz M., [in:] *Kodeks pracy. Komentarz*, ed. W. Muszalski, Warszawa 2019.

Suknarowska-Drzewiecka E., [in:] *Kodeks pracy. Komentarz 2020*, ed. K. Walczak, Legalis.

Tomaszewska-Michalak M., *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Warszawa 2015.

Torbus U., [in:] *RODO. Ochrona danych osobowych w zatrudnieniu ze wzorami*, ed. M. Mędrala, Warszawa 2018.

[34] According to the data minimisation principle, the controller may only process such types of data which are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. See A. Czarnowski, [in:] *RODO. Przewodnik ze wzorami*, ed. M. Gawroński, Warszawa 2018, p. 70.

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

Online sources

Article 29 – Data Protection Working Party, Working document in biometrics, Adopted on 1 August 2003, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf [access: 10.08.2021].

Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/57 [access: 7.02.2020].

Others

Decision of the Inspector General for Personal Data Protection of 23 September 2010, DIS/DEC-1133/37986/10.

Decision of the President of the Personal Data Protection Office of 18 February 2020, ZSZZS.440.768.2018.

Legal acts

Act of 26 June 1974 – Labour Code (consolidated text, Journal of Laws 2020, item 1320).

Act of 21 February 2019 amending certain other acts in order to ensure the application of 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 (Journal of Laws 2019, item 730).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, pp. 31–50).

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 (OJ L 119, 4.05.2016, pp. 1–88).

Case law

Judgement of the Supreme Administrative Court of 1 December 2009, I OSK 249/09, Legalis no. 332309.

ABSTRAKT

Z uwagi na wzrost popularności technik biometrycznych w praktyce można zauważyć pojawiające się wątpliwości dotyczące przesłanek warunkujących przetwarzanie danych biometrycznych. Przedmiotowe nieścisłości pojawiają się na gruncie różnych dziedzin prawa, w tym na gruncie prawa pracy. Niniejszy artykuł zawiera rozważania teoretyczne dotyczące przetwarzania danych szczególnej kategorii. Jego celem jest zwrócenie uwagi na potrzebę stworzenia odpowiednich regulacji prawnych służących zapewnieniu bezpieczeństwa przetwarzania danych biometrycznych pracowników oraz kandydatów do pracy. Artykuł rozpoczyna się od wyjaśnienia pojęcia danych biometrycznych oraz traktuje o praktycznych stronach wykorzystania narzędzi biometrycznych. W dalszej części autorka poddaje analizie regulacje prawne dotyczące przetwarzania danych biometrycznych w relacjach pomiędzy pracodawcą jako administratorem danych osobowych a pracownikiem jako podmiotem, którego dane są przetwarzane. W wyniku przeprowadzonych badań zaprezentowane zostało stanowisko wskazujące, że pracodawca przetwarzający dane biometryczne zatrudnionych pracowników oraz kandydatów do pracy powinien każdorazowo ustalać, czy dysponuje przewidzianą przez przepisy

Pobrane z czasopisma Studia Iuridica Lublinensia **http://studiaiuridica.umcs.pl**
Data: 20/11/2026 12:05:18

prawa przesłanką legalizującą przetwarzanie tych danych. Niniejszy artykuł jest jedną z niewielu prac w polskim dorobku piśmienniczym na temat przetwarzania danych biometrycznych. Głównym celem jest zaprezentowanie sytuacji, w których pracodawca może zgodnie z aktualnie obowiązującym stanem prawnym przetwarzać dane biometryczne swoich pracowników. Artykuł stanowi formę uniwersalnego przedstawienia problemu i może być przedmiotem zainteresowania zwłaszcza praktyków prawa.

Słowa kluczowe: biometria; dane biometryczne; prawo pracy; narzędzia biometryczne

UMCS