ANETA GIEDREWICZ-NIEWIŃSKA

# Protection of Employee Biometric Data

## Abstract

Biometric techniques can be used in the workplace to protect the interests of both employers and employees. They can help to adapt working conditions to employees' needs. Conversely, employers can use the processing of biometric data to implement workplace controls, particularly with regard to access to important information or sensitive areas. However, using biometric techniques can involve significant interference with privacy and other personal rights, posing a threat to the dignity of those concerned. This study aims to identify the privacy risks associated with processing employee biometric data. The discussion will focus on understanding what biometric data are and the current legal regulations on processing biometric data in an employment context.

KEYWORDS: employee, biometric bata, privacy, personal data, modern technology

ANETA GIEDREWICZ-NIEWIŃSKA – associate professor, University of Bialystok, ORCID – 0000-0003-0780-192X, e-mail: anetagiedrewicz@gmail.com

## 1 Introductory Remarks

Biometric technology is present in various areas of life and used for various purposes. In everyday life, it is mainly associated with unlocking a smartphone.[1] Two purposes can be identified for this technology. The first is to identify a person (i.e., to determine, on a speculative basis, who a person is). The second is to authenticate the person's identity (i.e., to confirm that the person has been identified correctly). Biometric technology is also one

1 The article is co-funded within the "Regionalna Inicjatywa Doskonałości" program of the Polish Ministry for Science and Higher Education.

HTTPS://DOI.ORG/10.36128/3YGWGQ22

of the modern methods used to manage employees. With the development of technology, biometric data are increasingly being processed in the working environment. In particular, employees' fingerprints, hand geometry and faces are processed using biometric techniques.

"Processing" means an operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) GDPR[2]).

From the employer's point of view, the processing of biometric data offers several benefits. It allows for an increase in the broader security of the workplace, and a reduction in the risk of fraud. This is because biometric data are characterised by uniqueness, which is very difficult to forge. There is no doubt that the level of security provided by biometric systems is much higher than that provided by badges, passwords, or personal identification numbers (PIN).[3] Despite its advantages, the use of biometric techniques involves interference with an individual's personal dignity and other personal rights, posing a significant threat to a person's privacy. This is particularly important because, under Article 47 of the Polish Constitution, every person has the right to the legal protection of his or her private life, family life, honour and good name, and to make his or her own personal choices. It must be emphasised that the right to privacy is a fundamental human right. Dignity, which is the foundation of all freedoms and rights, is linked to privacy. These terms are objectively related and intertwined.[4]

---

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2017 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 (Text with EEA relevance), Official Journal of the EU L. 119, p. 1, hereinafter: GDPR.

3 Chinchilla Rigoberto, "Ethical and Social Consequences of Biometric Technologies" *American Society for Engineering Education*, No 1 (2012): 5-6. https://peer.asee.org/ethical-and-social-consequences-of-biometric-technologies.pdf. [accessed: 15.5.2025].

4 See Constitutional Tribunal judgment of February 26, 2014, K 22/10, OTK 2014/2, p. 13.

The risks associated with the processing of biometric data should be treated with sensitivity.[5] It is crucial to search for legal solutions that can help create the proper balance between the interests of the employee and the employer. The employee will be interested in the legal protection of their privacy; for the employer, the control of the employee by means of biometric data is an important matter. The circumstances cited above support the view that the issue of processing employee biometric data is extremely topical and deserves to be fully addressed. The purpose of the study is to identify the privacy risks associated with the processing of employee biometric data. Achieving these objectives requires an understanding of what biometric data is, and the current shape of the legal regulation of biometric data processing in the employment context.

The primary responses to the risks associated with processing employee biometric data are the General Data Protection Regulation (GDPR) and the Labour Code. It is important to note that risks may also arise from the functioning of artificial intelligence when processing sensitive data. For example, this applies to compliance with the principle of data minimisation, the right of access to data, or doubts about the basis for processing to train AI models.

The widespread use of artificial intelligence algorithms in areas involving sensitive data required the creation of an appropriate legal framework. The use of modern technology has been regulated by Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).[6]

It is evident from the preamble to the Act on Artificial Intelligence (Article 10) that the principles of the aforementioned act and the General Data Protection Regulation (GDPR) are to be applied in their totality. Nevertheless, the obligations stipulated in the Act on Artificial Intelligence must be commenced on 2 August 2027. Consequently, the subject of this study will be the current legal regulations.

5 Günay Buket, "Biometrische Daten aus der Perspektive der DSGVO" *Datenschutz und Datensicherheit*, No. 2 (2023): 92.

6 Official Journal of the EU L. 2024/1689, hereinafter: Artificial Intelligence Act .

The formal-dogmatic method, also known as the dogmatic-legal method, will be used as the primary research tool.[7]

## 2 Biometric Data as Sensitive Data

Biometric data are data that every human being is born with. They belong to a special category of personal data (Article 9(1) GDPR). According to doctrine, representatives, the special nature of these data is demonstrated by the fact that they concern the privacy and even the intimate spheres, which entails a strong sense of risk and a danger of triggering discrimination in various areas, such as employment.[8] Biometric data are included in a closed catalogue of special categories of personal data.[9]

The President of the Office for the Protection of Personal Data (Poland) emphasises the following: "The biometric system identifies those characteristics which are, in principle, immutable and often (as in the case of fingerprint data) impossible to change. Due to the uniqueness and constancy of biometric data, which translates into their invariability over time, the use of biometric data should be carried out with particular care and caution. It should therefore be pointed out that a possible leakage of biometric data will result in a high risk of violation of the rights and freedoms of individuals."[10]

The creation of a definition of biometric data by the EU legislature is therefore to be welcomed. The literature on the subject rightly points out that "the introduction of a definition of biometric data and its recognition *expressis verbis* as sensitive data fills a gap, or even bridges a gap, in the legal regime for biometrics. This is dictated by the fact that the use of biometric

7 On methods of examining the law, see Tomasz Barankiewicz, "Metody myślenia, badania prawa i systematyzacji wiedzy w naukach prawnych," [in:] *Metodologia dysertacji doktorskiej dla prawników*, ed. Hubert Izdebski, Aneta Łazarska (Warszawa: Wolters Kluwer, 2022), 113.

8 Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, *Ochrona danych osobowych. Komentarz* (Warszawa: Wolters Kluwer, 2015), 569.

9 Article 9 (1) GDPR. On the concept of biometric data more extensively, see Sylwia Zaborska, "Legal Regulation of the Protection of Biometric Data under the GDPR" *Studia Iuridica Lublinensia*, Vol. XXVIII (2019): 100-102.

10 Decision of the President of the Personal Data Protection Office ZSZZS.440.768.2018 (Poland).

techniques involves a profound intrusion into the privacy of the person whose data is being processed."[11] According to the definition, these include personal data that result from specific technical processing; concern the physical, physiological or behavioural characteristics of a natural person; and allow or confirm the unambiguous identification of that person, such as facial image or dactyloscopic data (Article 4(14) GDPR). As can be seen from the definition above, there are two categories of biometric data: (1) physical, physiological characteristics, which are derived from a person's unique physical attributes, including fingerprints, hand or facial geometry, iris image, the vascular pattern of the hand or finger, and (2) behavioural characteristics, which are derived from a person's behavioural patterns, such as voice timbre, the way they move, or the way they hit a keyboard.[12]

In the definition of the term "biometric data" provided by the GDPR, there is an element of "personal data that allows or confirms the unequivocal identification of that person." It presupposes the disclosure of one's identity through tools, rather than directly from data. For example, a person's fingerprint or internet protocal address (IP) data make it possible to identify them. Modern technologies play a special role in identification. The EU legislature explicitly indicates, in the definition of biometric data, that these are personal data that result from "special technical processing" (i.e., processing using biometric techniques).

In light of the above regulation, not all information relating to a person's physical, physiological, or behavioural characteristics can be counted as biometric data.[13] This is well illustrated by the facial image, which is explicitly categorised by the EU legislature as biometric data. However, it should be borne in mind that not every photograph containing a facial

11 Urszula Torbus, "Dane szczególnie chronione w stosunkach pracy," [in:] *RODO. Ochrona danych osobowych w zatrudnieniu ze wzorami*, ed. Małgorzata Mędrala (Warszawa: Wolters Kluwer 2018): 96; Anna Dmochowska, "Przetwarzanie danych szczególnych kategorii," [in:] Anna Dmochowska, Marcin Zadrożny, *Unijna reforma ochrony danych osobowych. Analiza zmian* (Warszawa: C.H. Beck, 2016), 29; Ewa Kulesza, "Podstawowe pojęcia z zakresu danych osobowych,", [in:] *Ochrona danych osobowych w zatrudnieniu*, ed. Dominika Dörre-Kolasa (Warszawa: C.H. Beck, 2020), 30.

12 Cristina Dell Rosso, "Access Granted: An Examination of Employee Biometric Privacy Laws and a Recommendation for Future Employee Data Collection" *Journal of Law, Economics & Policy*, No. 1 (2023): 26.

13 Magdalena Kuba, "Komentarz do art. 4 pkt 14 RODO", [in:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, ed. Edyta Bielak-Jomaa, Dominik Lubusz (Warszawa: Wolters Kluwer, 2018), 276-277.

image is biometric data.[14] According to recital 51 of the GDPR, a facial photograph can only be considered biometric data if it is processed by specific technical methods that allow for the unambiguous identification of the natural person or the verification of his or her identity. This is the case when a photograph or other material medium in which a recognisable likeness of a human face is recorded is processed using automated facial recognition technology.[15]

Automatic face recognition is a technology that uses an automated mechanism to recognise people based on facial image analysis. Algorithms detect the face in the image (a photo or recording). Then, the features of the face are determined, and the next stage is the recognition or non-recognition of the person as a result of comparing the determined features with a model base. Regarding the technical aspect of this process, direct contact with the person being potentially recognised and interaction with them are not necessary. It is therefore possible to use this technology "from behind the scenes," without having to inform the recognised person.[16]

Biometric data processing is based on the use of information that is, in principle, immutable and unique to a specific individual. This means that, once acquired, an individual's data will not become obsolete and cannot be changed by the data subject himself as easily as other personal data (e.g., a telephone number or residential address). In addition, some biometric data are based on characteristics that only change in exceptional situations, such as an accident or injury. These characteristics include fingerprints and retinal images.

Biometric recognition systems are becoming more widespread and diverse. As technology advances, their power and scope of influence will increase. This raises questions about the extent of the potential intrusion into the private lives of individuals. This is particularly evident when biometric technologies are part of a control and surveillance system. There

14 Paweł Fajgielski, "Automatyczne rozpoznawanie twarzy – wybrane zagadnienia prawne," [in:] *Prawo sztucznej inteligencji i nowych technologii*, ed. Bogdan Fischer, Adam Pązik, Marek Świerczyński (Warszawa: Wolters Kluwer, 2021): 83.

15 Remigiusz Lewandowski, "Alternatywne narzędzia zdalnej identyfikacji" *Przegląd Bezpieczeństwa Wewnętrznego*, No. 25 (2021): 96-98; Joanna Haberko, Krzysztof Niziołek, „Wykorzystanie algorytmów sztucznej inteligencji w rozpoznawaniu twarzy w celu określenia podobieństwa fenotypowego w procedurach medycznie wspomaganej prokreacji *Białostockie Studia Prawnicze*, No. 1 (2025): 241.

16 Fajgielski, "Automatyczne rozpoznawanie twarzy – wybrane zagadnienia prawne," 79.

is a risk of a breach affecting an employee's biometric data, which can be increased by the nature and extent of the data collected by an employer.

The use of advanced technology does not exclude the fact that the processing of biometric data may be performed in error. Errors occur in many areas. For example, they can occur when the images analysed show the same person at various ages. In addition, some systems have better results for white-skinned people than dark-skinned people, as well as better results for men than women, and better results for adults than teenagers. This can lead to discrimination. The processing of personal data also carries other risks. For example, data blackmail, computer fraud, false data entry, false identification and identity theft (e.g., CEO impersonation) may occur.

The risks that are incurred by implementing biometric security often include the incorrect storage of data taken from users of a particular system, which are used for authentication. If, as a result of a cyberattack, hackers gain access to the passwords we use to log into a business account, for example, we can change them. Biometric security does not give us this option. We cannot change the retinas in our eyes or the fingerprints on our fingertips. These risks will affect both the person who processes the personal data and the person who provided the data for processing. In the former case, the largest perceived threat will be penalties for non-compliance with the GDPR, and, in such cases, a negative impact on people's rights.[17] This, in turn, may result in complaints, unpleasant comments on the Internet, a bad reputation for the companies processing biometric data, or legal proceedings.

## 3 Rationale for Processing Biometric Data in the Polish Labour Code and the GDPR

The GDPR provides a legal framework that encourages responsible innovation. Article 9(1) of the GDPR contains a catalogue of specific data, among which are biometric data. The special nature of biometric data makes the processing of such data generally prohibited (Preamble of the GDPR,

17 Magdalena Tomaszewska-Michalak, *Prawne i kryminalistyczne aspekty wykorzystania technologii biome-trycznej w Polsce* (Warszawa: Difin, 2015), 191.

recital 51). This prohibition does not apply, only if the conditions strictly defined by the aforementioned regulation are met (Article 9(2)). Prerequisites such as the protection of the vital interests of a natural person, important public interests, and public interests in the field of public health play an important role in the processing of biometric data.

The role of the obligation to assess the impact on data protection (Article 35 of the GDPR) should also be emphasised. Importantly, this requirement must be fulfilled before data processing begins, i.e. at the stage of planning, designing processing systems and implementing solutions. This is a specific obligation, not a general one, as it only applies to types of processing that may involve high risk. The purpose of this legal construct is to adopt appropriate safeguards in the form of solutions that take into account the risks associated with data processing.[18] According to the position of the Data Protection Agency (DPA), the above assessment is mandatory in the case of processing biometric data for the purpose of identifying a natural person, or for control purposes.[19] The above regulations are also applicable in the area of employee data protection.

However, Article 88(1) of the GDPR contains a clause authorising a Member State to adopt "more detailed provisions" to ensure the protection of rights and freedoms when employees' data are processed in connection with employment. As stated by the Court of Justice of the European Union (CJEU) in its judgment of 30.03.2023 in Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums,[20] a national regulation cannot constitute a "more detailed provision" if it does not meet the conditions set out in paragraph 2 of Article 88 of the GDPR. It follows from Article 88(2) that these regulations cannot be limited to a repetition of the provisions of the regulation and should aim to protect the rights and freedoms of employees when their personal data are processed in connection with their employment,

18 Arwid Mednis, „Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych," [in:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, ed. Grzegorza Sibiga (Warszawa: C.H. Beck, 2016), 31.

19 Personal Data Protection Office, *Kiedy trzeba przeprowadzić ocene skutków dla ochrony danych? z 2025 r.* www.uodo.gov.pl. [accessed: 15.5.2025].

20 Court of Justice judgment of March 30, 2023, in Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v Minister des Hessischen Kultusministeriums, Case C-34/21.

and include appropriate and specific measures to ensure that the data subject's dignity, legitimate interests and fundamental rights are respected.

In Polish law, such national solutions include Articles $22^1$, $22^{1a}$ and $22^{1b}$ of the Labour Code. These provisions provide for two prerequisites authorising an employer to process biometric data. The first prerequisite is the consent of the employee (the applicant for employment), provided that the transfer of the data was initiated by that person. The second prerequisite is the need to ensure control of access to particularly important information, the disclosure of which may expose the employer to damage, or access to premises in the workplace requiring special protection.[21] The processing of biometric data on the basis of consent is only possible, as the DPA confirms, when those data have been provided by the candidate (employee) on their "own initiative."

The Polish legislature's emphasis on the provision of biometric data on the initiative of the job candidate (employee) serves, in my opinion, to demonstrate the subsequent voluntariness of the processing of such data. Indeed, it is difficult to speak of voluntary consent in an employment relationship, the essence of which presupposes an imbalance in power between the data subject and the controller.[22] A refusal by an employee to give consent to an employer for processing is unlikely, given the relationship that exists between the two. Consent is not voluntary when there is any element of coercion or pressure involved.[23]

The legislature does not define what is to be understood by the term "on one's own initiative." In my opinion, it would be desirable, in the future, for

21 Kazimierz Jaśkowski in: *Komentarz aktualizowany do kodeksu pracy*, ed. Kazimierz Jaśkowski, Eliza Maniewska (Lex, 2025); Magdalena Kuba In *Kodes pracy.* Komentarz, t. I, *Art. 1-93*, ed. Krzysztof W. Baran (Lex, 2025); Małgorzata Gersdorf, Michał Raczkowski in: Wojciech Ostaszewski, Krzysztof Rączka, Agnieszka Zwolińska, Małgorzata Gersdorf, Michał Raczkowski, *Kodeks pracy. Komentarz* (Lex, 2024).

22 Only in exceptional circumstances can employees seemingly give their voluntary consent. In such cases, their giving or not giving consent has no negative consequences. For example, such a situation arises when a film crew intends to film in a particular part of an office and the employer asks all employees sitting in that part to consent to filming, as their image could appear in the film, in the background. Those who did not want to be filmed did not suffer any negative consequences, and were given similar desks in the same place in the building for the duration of the filming. Guidelines 05/2020 of the European Data Protection Board of 4 May 2020 on consent under Regulation 2016/679. www.edpd.europa.eu. [accessed: 15.5.2025].

23 Decision of the President of the Personal Data Protection Office, 13.07.2022 r., D.S. 523.7988.2021.

the President of the DPA to clarify how the phrase "on one's own initiative" is to be interpreted. In the practice of biometric data processing, this may lead to ambiguity. The prevailing view in the literature is that there cannot be a transfer of data on the employer's initiative in such a situation.[24] According to this position, an employer cannot "go out on a limb" regarding the processing of biometric data, even when employees fully accept and support this. If one were to take the above position strictly, any action on the part of the employer would be excluded. However, given the current state of the law, it seems that the above-mentioned premise is also fulfilled if the employer (a) merely informs the employees about a certain internal initiative, and the employee joins it voluntarily by providing his or her sensitive data, or (b) asks a question about sensitive data, to which the employee's answer is voluntary. Excluding the possibility of any encouragement by the employer seems to lead to too narrow an interpretation of the phrase "on their own initiative."

For the processing of specific data, the DPA requires "explicit consent" (Article 9(1)). The European Data Protection Board's (EDPB's) 05/2020[25] guidance on the issue of "explicit consent" clarifies that an "unambiguous" demonstration of intent in the form of a "statement or clear affirmative action" is necessary, in line with previous guidance issued by the Article 29 Working Party[26]. "Explicit affirmative action" implies that the data subject must have taken a deliberate action to consent to the specific processing performed. Recital 32 provides further guidance in this regard. Consent can be obtained using a written or (recorded) oral statement, including electronically. Perhaps the most literal way to meet the 'written statement' criterion is to ensure that the data subject sends a letter or email to the controller explaining exactly what he or she agrees to. Written declarations can take a variety of forms and sizes that comply with the GDPR. Without prejudice to existing (national) contract law, consent can be obtained in the form of a recorded oral statement, although the information available to the data subject must be properly taken into account before consent is given. The use of pre-ticked boxes for consent is invalid under the GDPR. Silence

24 Joann Jarguz in: *Kodeks pracy. Komentarz*, ed. Arkadiusz Sobczyk (Legalis, 2023); Ewa Suknarowska-Drzewiecka in: *Kodeks pracy. Komentarz*, ed. Krzysztof Walczak (Legalis, 2025).

25 Guidelines 05/2020 of the European Data Protection Board of 4 May, 2020 on consent under Regulation 2016/679. www.edpd.europa.eu. [accessed: 15.5.2025].

26 Guidelines of the Article 29 Working Party of 10 April, 2018 on consent under Regulation 2016/679 (WP259.1).

or inaction on the part of the data subject, as well as simply continuing to use the service, cannot be considered an active indication of choice.

In addition, consent should be "explicit," and this, according to the abovementioned guidelines, refers to how the data subject gives their permission. This can occur in the form of either the confirmation of consent in a written statement, or the signing of a written statement by the data subject. However, such a signed statement is not the only way to obtain explicit consent. For example, in a digital or online context, a data subject may make the required statement by filling out an electronic form, sending an email, sending a scanned document bearing the data subject's signature, or providing an electronic signature.

In the opinion of the President of the Office for Harmonisation in the Internal Market (OHIM), the content of the above-mentioned EDPB's guidelines indicates that an oral declaration of consent to data processing, both in the case of "ordinary" data and, even more so, in the case of "specific" data, is not a form that sufficiently guarantees the demonstration of the unambiguity, let alone the clarity, of the consent given. Such a form, in the case of "ordinary" data, could be considered sufficient, especially if it is followed by other additional steps by the controller (e.g. by drawing up an appropriate consent register or audio-recording conversations with data subjects).[27]

The candidate's (employee's) consent, preceded by the person's initiative, for the processing of biometric data is not needed when the provision of such data is necessary to control access to sensitive information, the disclosure of which could expose the employer to damage (e.g., technological), or access to premises requiring special protection (e.g., the storage of a work of art). In such a situation, it can be assumed that the employer's right to process biometric data stems from the employee's duty to take ensure the welfare of the workplace, protect its property, and keep secret any information the disclosure of which could expose the employer to harm.[28] Against the backdrop of the above rationale, the question arises as to whether biometrics can be used in time management. In a guide on attendance control with biometric systems, the Spanish Data Protection

27 Decision of the President of the Personal Data Protection Office, 30.11.2022 r., DKN.5112.5.2021.

28 Joanna Jarguz in: *Kodeks pracy. Komentarz*, ed. Arkadiusz Sobczyk (Legalis, 2023).

Agency (AEPD – Agencia Española de Protección de Datos) analysed the legal basis for using such systems.[29]

According to the agency, the right to use biometrics to record working time can be derived from Article 9(2)(b) of the GDPR, which allows the general prohibition against processing specific data to be lifted if there is a corresponding national provision. This means, in the agency's view, that a necessary condition is the presence, in the Member State concerned, of a regulation with the force of law that explicitly authorises such use of biometric data. The AEPD has accepted the notion that the consent of the employee cannot constitute a legal basis for the processing of biometric data for time management at work. Consent is not voluntary. This is due to the imbalance between the parties involved in the employment relationship.

In 2018, the President of the Data Protection Authority in Poland made it clear that the processing of employees' biometric data by an employer cannot be used to record working time.[30] The employer was considered to have other methods available to investigate an employee's attendance at work. In the opinion of the Polish Office, taking biometric data from employees does not serve the purpose of recording working time, but rather that of restricting access to places that are particularly protected for some reason. The employer cannot demonstrate why it uses biometric data monitoring for work attendance. Like the Spanish supervisory authority, the Polish Authority also ruled out the possibility of processing an employee's biometric data for time-recording purposes based on the employee's consent. In doing so, he referred to a 2009 judgment[31] in which the Supreme Administrative Court questioned the voluntariness of consenting to the collection and processing of biometric data due to an imbalance in the employee–employer relationship.

However, controversially, some believe that the dynamic development of modern technology should lead to a re-examination of the current position on processing biometric data in the employment area. It is seen that the

29 Agencia Española Protección Datos, Guía sobre tratamientos de control de presencia mediante sistemas biométricos. www.aepd.es. [accessed: 15.5.2025].

30 Personal Data Protection Office, *Poradnik o przetwarzaniu danych przy zatrudnianiu "Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców" z 2018 r.* www.uodo.gov.pl. [accessed: 15.5.2025]; Martyna Betiuk, „Czy biometryczne ewidencjonowanie czasu pracy pracownika jest zgodne z rozporządzeniem 2016/679?" *Doradztwo Podatkowe*, No. 12 (2022): 32.

31 Supreme Administrative Court judgment of 1 December 2009, I OSK 249/09, ONSAiWSA 2011, No. 2, item 39.

previous position on time recording using biometric data is not in line with market practice and current technological developments. Furthermore, the argument that an employer should not use new technology if older solutions are doing their job blocks development, according to practitioners.

## 4 Summary

Modern technologies create many opportunities in many sectors of society, including employment. On one hand, they make it easier to carry out paid work and control how it is carried out; on the other hand, the use of new technologies generates threats to the employee's right to privacy. These risks are visible when the employer controls the performance of work by processing special categories of personal data, such as biometric data. There is no doubt that even innovative proposals, such as monitoring an employee's emotional states during the performance of daily work duties (a brain-computer interface [BCI] system[32]), entail a significant intrusion into the employee's privacy. Similarly, the collection of data on individuals' DNA may carry the risk of its misuse for purposes of employment discrimination, in which an employer refuses to hire a job applicant because the prospective employee is likely to contract cancer or other diseases.

Many regulations create boundaries that protect individual rights and freedoms from undue interference. This certainly poses some challenges that any employer must face when considering the introduction of biometrics. These regulations include, first and foremost, the provisions of the GDPR. They contain principles for the collection and processing of personal data that affect the interpretation of national regulations. These principles are particularly relevant, especially in the case of sensitive data, such as biometric data. Undoubtedly, in the case of biometric data, the fundamental principle is that of data minimisation. According to this principle, the data processed must be adequate, relevant, and limited to only what is strictly necessary for the purposes specified (Article 5 GDPR). Thus, employers should search for alternative, less intrusive methods to achieve the intended purpose. The processing of biometric data requires

32 Karolina Trzyniec, "Monitorowanie stanów emocjonalnych pracownika za pomocą interfejsów mózg-komputer," *Bezpieczeństwo Pracy*, No. 12 (2017): 23-25.

a good justification, based on both a risk analysis and a data protection impact assessment. Necessity and proportionality requirements must be considered. It may turn out, after an assessment of the employer's existing data-processing systems, that they can be improved without the introduction of biometrics.

The provisions of the GDPR and national law are complementary. The above prerequisites for the processing of biometric data contained in the Polish Labour Code raise questions in practice. They should be applied in compliance with the principles indicated in the GDPR, in particular the principle of data minimisation. In practice, this means that the processing of biometric data is not necessary for working time management.

## Bibliography

Barankiewicz Tomasz, „Metody myślenia, badania prawa i systematyzacji wiedzy w naukach prawnych," [in:] *Metodologia dysertacji doktorskiej dla prawników*, ed. Hubert Izdebski, Aneta Łazarska. 101-129. Warszawa: Wolters Kluwer, 2022.

Barta Janusz, Paweł Fajgielski, Ryszard Markiewicz, *Ochrona danych osobowych. Komentarz*. Warszawa: Wolters Kluwer 2015.

Betiuk, Martyna. „Czy biometryczne ewidencjonowanie czasu pracy pracownika jest zgodne z rozporządzeniem 2016/679?", *Doradztwo Podatkowe*, No. 12 (2022): 30-33.

Chinchilla Rigoberto, „Ethical and Social Consequences of Biometric Technologies" *American Society for Engineering Education*, No. 1 (2012): 1-10. https://peer.asee.org/ethical-and-social-consequences-of-biometric-technologies.pdf.

Dell Rosso Cristina, „Access Granted: An Examination of Employee Biometric Privacy Laws and a Recommendation for Future Employee Data Collection" *Journal of Law, Economics & Policy*, No. 1 (2023): 24-50.

Dmochowska Anna, „Przetwarzanie danych szczególnych kategorii," [in:] Anna Dmochowska, Marcin Zadrożny, *Unijna reforma ochrony danych osobowych. Analiza zmian*. 28-40. Warszawa: C.H. Beck 2016.

Fajgielski Paweł, „Automatyczne rozpoznawanie twarzy – wybrane zagadnienia prawne," [in:] *Prawo sztucznej inteligencji i nowych technologii*, ed. Bogdan Fischer, Adam Pązik, Marek Świerczyński. 77-91. Warszawa: Wolters Kluwer, 2021.

Günay Buket, „Biometrische Daten aus der Perspektive der DSGVO" *Datenschutz und Datensicherheit*, No. 2 (2023): 96-99. https://doi.org/10.1007/s11623-023-1724-x

Haberko Joanna, Krzysztof Niziołek, „Wykorzystanie algorytmów sztucznej inteligencji w rozpoznawaniu twarzy w celu określenia podobieństwa fenotypowego w procedurach medycznie wspomaganej prokreacji" *Białostockie Studia Prawnicze*, No. 1 (2025): 241-261.

*Kodeks pracy. Komentarz*, ed. Arkadiusz Sobczyk, Legalis, 2023.

*Kodeks pracy. Komentarz*, ed. Krzysztof Walczak. Legalis, 2025.

*Kodes pracy.* Komentarz, t. I, Art. *1-93*, ed. Krzysztof W. Baran. Lex 2025.

*Komentarz aktualizowany do kodeksu pracy*, ed. Kazimierz Jaśkowski, Eliza Maniewska. Lex, 2025.

Kuba Magdalena, „Komentarz do art. 4 pkt 14 RODO", [in:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, ed. Edyta Bielak-Jomaa, Dominik Lubusz. 273-277. Warszawa: Wolters Kluwer, 2018.

Kulesza Ewa, „Podstawowe pojęcia z zakresu danych osobowych", [in:] *Ochrona danych osobowych w zatrudnieniu*, ed. Dominika Dörre-Kolasa. 30-40. Warszawa: C.H. Beck 2020.

Lewandowski Remigiusz, „Alternatywne narzędzia zdalnej identyfikacji" *Przegląd Bezpieczeństwa Wewnętrznego*, No. 25 (2021): 85-101.

Mednis Arwid, „Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych," [in:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, ed. Grzegorza Sibiga. 31-40. Warszawa: C.H. Beck 2016.

Ostaszewski Wojciech, Krzysztof Rączka, Agnieszka Zwolińska, Małgorzata Gersdorf, Michał Raczkowski, *Kodeks pracy. Komentarz*. LEX, 2024.

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

Torbus Urszula, „Dane szczególnie chronione w stosunkach pracy", [in:] *RODO. Ochrona danych osobowych w zatrudnieniu ze wzorami*, ed. Małgorzata Mędrala. 95-100. Warszawa: Wolters Kluwer 2018.

Trzyniec Karolina, „Monitorowanie stanów emocjonalnych pracownika za pomocą interfejsów mózg-komputer" *Bezpieczeństwo Pracy*, No. 12 (2017): 23-25.