*DOI:10.35774/app2023.03.030*
*UDC 341.1/.8*

***Daria Bulgakova,***
*Doctor of Laws, Ph.D. in International Law, Visiting scholar, researcher, Law Department, Uppsala University, Sweden, Advocate, Dnipropetrovs'k Regional Bar Council,Ukrainian National Bar Association Member*
*ORCID: https://orcid.org/0000-0002-8640-3622*

***Valentyna Bulgakova,***
*Pedagogue-Methodist of the Highest Category, Supervisor of Scientific Manuscripts, Kryvyi Rih, Ukraine*
*ORCID: https://orcid.org/0009-0009-6463-5228*

# THE PRACTICE OF ARTIFICIAL INTELLIGENCE FOR THE TIME-ATTENDANCE DETECTION IN A WORKSTATION

*The research emphasizes the importance of applying theoretical knowledge in legal practice, especially concerning the notion under General Data Protection Regulation (GDPR) Article 9 when legislator, according to paragraph 2, has allowed the use of artificial intelligence based on exceptions provided in «a» and «b» from the prohibition rule under paragraph 1 of the mentioned provision. Due to that, research reveals legal relations concerning unique identification practices in the workplace. Two kinds of legal relations are targeted as examples. The first one involves the time management of employees at the workplace, where the application of the principle of proportionality exemplifies that unique identification can only be practiced if there is a strict necessity. The second one discussed in terms of regulations for implementing devices that use biometric authentication for the access control to premises in workplaces under consent given by the employee.*

*The research confirms that unique identification in the workplace is acceptable under Article 9 (2, a & b) of the GDPR, but interference with the fundamental right of an employee to the personal data protection in a workstation for unique identification must be legitimate and proportionate to the terms to derogate from the GDPR Article 9 (1). The research suggests installing the advancement of operative interfaces and experienced technology with non-biometric intelligent systems that can deliver ample time tracking in the workplace.*

***Keywords:*** *GDPR, smart technology, unique identification of employees, the right to personal data protection, consent.*

***Булгакова Д. А., Булгакова В. А.***

***Практика застосування технологій зі штучним інтелектом для обліку робочогу часу на робочому місці***

*Дослідження підкреслює важливість застосування теоретичних знань у юридичній практиці, особливо щодо поняття, передбаченого ст. 9 Загального Регулювання Захисту Даних (GDPR), коли законодавець відповідно до ч. 2 дозволив використання штучного інтелекту на основі винятків, передбачених пунктами «а» і «b» із правила заборони за ч. 1 зазначеного положення. У зв'язку з цим у дослідженні виявлено правовідносини, пов'язані з практикою унікальної ідентифікації на робочому місці.*

*Як приклади розглядаються два види правовідносин. Перший пов'язаний з управлінням часом працівників на робочому місці, де застосування принципу пропорційності показує, що унікальна ідентифікація може застосовуватися лише в разі суворої необхідності. Другий розглядається з точки зору регулювання впровадження пристроїв, що використовують біометричну автентифікацію для контролю доступу до приміщень і розумних додатків, встановлених на робочих місцях за наданою згодою працівника.*

*Результати дослідження показують, що визначення часу присутності працівників на робочому місці через застосування технологій зі штучним інтелектом варто переглянути, щоб оцінити переваги та ризики, пов'язані з цим.*

*Дослідження підтверджує, що унікальна ідентифікація на робочому місці прийнятна згідно зі ст.. 9 (2,*

*a & b) GDPR, але втручання у фундаментальне право робітника на захист персональних даних під час обробки біометричних даних має бути законним і пропорційним необхідності відступу від ст.. 9 (1) GDPR. У дослідженні наголошено на важливості надання гарантій працівнику щодо доступу до персональних даних та без затримок, а також необхідності роботодавцю обмежити доступ до бази даних третім особам.*

*Дослідження попереджає, що нехтування роботодавцем організаційними та технічними процедурами резервного захисту не дозволяє повною мірою оцінити ризики і може призвести до недостатнього захисту персональних даних працівника.*

*Дослідження рекомендує проводити міждисциплінарні дослідження щодо використання біометричних характеристик розумними автоматизованими методами та закликає до прийняття нормативно-правових актів, які забезпечують прозору, цілеспрямовану та зрозумілу практику застосування штучного інтелекту для громадян, які не є фахівцями-юристами, зокрема для роботодавців та працівників.*

*Запропоновано приділити увагу до вдосконалення операційних інтерфейсів і важливості перевірки того, чи можуть небіометричні системи технологій зі штучним інтелектом забезпечити достатній облік часу на робочому місці.*

***Ключові слова:*** *GDPR, смарт-технології, унікальна ідентифікація працівників, право на захист персональних даних, згода.*

**Introduction.** The fast growth of information technology has increased the need for robust personal data protection, which the European Union (EU) provides. Protecting this right has become more challenging as technology advances, especially with the widespread use of digital biometric technology in the business sector. The risks for individuals' unique characteristics and the EU's legal framework face new challenges in regulating it. The Regulation (EU) 2016/679 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) (GDPR) has made significant progress in protecting personal data, including biometric data processed by Artificial Intelligence (AI). However, there is controversy enclosing the practice of AI in the employment context, which is the research's focus.

Transparency is a fundamental principle of personal data processing under GDPR Article 5 (1) (a). It is closely linked to the principles of reasonableness and legality when collecting personal data from data subjects, which means companies must provide information following GDPR Article 13. Providing adequate information to employees (data subjects) is crucial to ensure they can make informed decisions and understand the implications of their consent. While Article 13 does require that certain information shall be provided to data subjects at the time of approval, it is essential to note that a valid license may not always be subject to this condition. This information must still be available to data subjects in other ways, such as through the company's privacy notice. To obtain a valid consent, the employer (data controller/processor) must provide the data subjects with specific information, including (i) their identity, (ii) the purpose of processing, (iii) what data will be collected and used, (iv) the right to withdraw consent, (v) any use of automated decision-making under Article 22, where relevant, and (vi) any risks associated with international data transfers in the absence of adequate safeguards. By providing this information, data subjects can make informed decisions about whether to provide consent relying on transparent and responsible AI practice in the workstation.

According to GDPR Article 6 (1) (a), consent must be given for one or more specific purposes. Valid consent requires several conditions to be met. One of these is the identification of the consent itself. To identify consent, a company must (i) determine and specify the intended purposes, (ii) provide explicit requests for separate consent if necessary, and (iii) differentiate consent from other related information. In practical application situations, the individuality of consent is generally less challenging than voluntary consent. In an employment relationship where automatic processing is used, identifying the specific purposes for each use case is relatively straightforward. Transparent information is crucial to ensure that employees understand the purpose for which their data is being used, and it is vital for valid consent.

**Analysis of recent research and publications.** Only a few researchers have studied the appointed theme of the research, which demands more attention from the scientific community of law. As it has been found, installing biometric systems in a workplace should not abuse employee data protection. Employers cannot impose restrictions on worker rights [2, p. 34]. Since the deployment of a biometric system is usually carried out for all employees, it can extend its use to a limited number of data subjects [2, p. 34].

According to scholar Cefaliello [4], the term «data» mentioned in Article 9 of the GDPR refers to personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data to uniquely identify an individual, data concerning health, or data

concerning a person's sex life or sexual orientation. These categories are some grounds against which employees cannot be distinguished. The processing such special personal data is not permitted unless one of the following exceptions applies: (1) the (prospective) employee gives a consent (as outlined in Article 7(3)(a) of the GDPR) (2) the employer exercises rights and obligations under labour or social law and fulfils legal obligations (as outlined in Article 7(3)(b) of the GDPR), or (3) the (prospective) employee makes personal data publicly available to others where, significantly, the shared private information may not always be relevant to fulfilling the employment contract.

In this respect, Sowa et al. [11] in findings present that AI in the field of employment should prioritize collaborative approaches between humans and leads to increased productivity in knowledge work rather than complete automation. Also, a scholar Upchurch [12] examines debates and controversies around the impact of robots and AI on the world of work and reflecting outcome on Alan Turing's tests of artificial intelligence and their efficacy in modern applications. The study concludes that technological singularity is not imminent and examines aspects of public policy. Scholars tend to support prioritizing frontline employees (FLEs) roles in hospitality services and expect AI to empower those roles where engaged FLEs are the primary sources of human-centered hospitality and interactions; authentic hospitality perceived by customers is a service outcome of FLEs with proactive inputs of physical and psychological resources [10].

Consequently, according to Kassir et al. [7], the current discourse on innovations in employment selection is flawed for two reasons: (1) it ignores the fact that large corporate employers seldom rely solely on human decision-making and often use traditional hiring tests, and (2) it fails to consider the benefits of recent technological advancements in light of the domain-specific challenges of employment selection that have sustained the «diversity–validity dilemma». These various spatial developments, representing reduced control by office workers of their immediate working environment, seem more likely to be found in large-scale routine back-office work where there is little face-to-face contact with the public or customers [5]. However, Weiss [13] suggests that using employee data in a job application may increase the opposing perspectives of the applicant, but not more than if they received assistance from a human.

**Statement of the problem.** According to the GDPR Article 9 (1), unique identification is prohibited; however, companies can escape from such strictness when there is a relevant «abnormality» under paragraph 2. Consent as a basis for legitimizing the use of AI in an employment relationship as per GDPR Article 9 (2, a & b) can be misleading and problematic due to the unequal power dynamic between employers and employees. While obtaining voluntary consent is not entirely excluded, it should only be used when the employee has a genuine choice, and their consent can be withdrawn without adverse consequences.

The lack of specific legislation poses a challenge for employers who want to implement intelligent identification systems in the workplace since biometric data is categorised as susceptible personal data under the GDPR. Employers must navigate the thorny question of whether and how to allow the practice of smart technology to process employees' data complying with the GDPR while also considering the benefits of such techniques for their business activities. In this regard, the research interest of Article 9 (2) of the GDPR primarily relies on two exceptions. Firstly, it is explicit consent from the data subject under (a): «the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject». Secondly, it is unique identification in employment context under (b) which specifies that «processing is necessary for carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject».

**The purpose of the research article** addresses the exploration of whether explicit consent could be sufficient for using intelligent technology with biometric techniques in the workstation and whether the additional settings need to be altered. The research target is to find out finding the most common practice of biometric data processing in workstations and develop recommendations for compliant framework.

**Methodology.** The research examinates the legal mechanism of the principle of proportionality application on stipulations regarding the use of AI with biometric techniques under the GDPR Article 9 (2, a & b). This approach provides critical insights into emerging paradigms and practices of AI in workstations.

The research design is structured into three stages. These stages are complemented by a forward-looking analysis of the goals, drivers, barriers, and risks associated with the AI's use in the workplace, including :

1) analysing the data protection implications of AI usage in workstations;

2) investigating the complementarities between biometric data and companies' data governance processes;

3) assessing which AI practices best support employee trust and strengthen unique identification legitimacy [8, p. 2].

Accordingly, the article offers inputs for a landscaping exercise of AI governance together with the data regulatory frameworks in the EU, drawing from the GDPR to the experiences of France and Sweden.

**Research results.** The EU promotes synergies between individuals and companies where the accuracy of biometric technology is beneficial. The application of proportionality principle to use biometric technology in various scenarios, such as access control, time tracking, and logging into workstations and applications, is critical. Employers must determine in advance whether smart technology for unique identification of employees is necessary, consider the legal risks associated with processing employees' unique characteristics and apply proportionality criteria to ensure compliance with data protection regulation.

*Table 1*

**Legal Criteria of the Principle of Proportionality for Biometric Data Processing Application**

| Steps | Disadvantage | Benefit | Aim | Result |
|---|---|---|---|---|
| | Risks | Proportionality | Biometric Data Processing | Compliance |
| 1 | Uncertainty on the Necessity | Legitimacy | GDPR Article 9 (1) (2) + Recital 4 | + |
| 2 | Incompatible Interests | Balance of Interests | Lawfulness GDPR Article 6 (1, a) | + |
| 3 | Other Purpose then Initially Established | Limitation & Determination | Processing under Control of a Person involved in the Legal Relationship concerning him/her Biometric Data | + |
| 4 | Disclosing other categories of Data, and Processing for Incompatible Purposes | Ensuring Legal Protection | Technical and Organizational Measures | + |

Source of a Table «Legal Criteria of the Principle of Proportionality for Biometric Data Processing Application»: Bulgakova, D. (2021). Application of the Principle of Proportionality on Biometric Data Processing in European Union Law. University of International Business and Economics (UIBE), Law Faculty, Doctoral of Laws Degree Dissertation, p. 150.

Under the table «Legal Criteria of the Principle of Proportionality for Biometric Data Processing Application» [1], the proportionality steps consist of four logical criteria to meet the GDPR' Article 9 (1) (2, a & b) requirements. Based on that, before implementing biometric technology, its necessity must be evaluated. Hence, the research proposes concentrating explicitly on necessity for intelligent approaches to detect employee attendance by applying proportionality criteria in practice. The necessity criterion is a precondition for a proportionality, and other standards are irrelevant if necessity is not met. To address uncertainty regarding the necessity, the GDPR Article 9(1) (2, a & b) provides a legal ground for applicable standard with reference to the legitimacy. To obtain permission to process biometric data, employment relationships shall extent data protection policy.

In the context of the employment relationship, to evaluate whether biometric identification is necessary for the intended purpose and whether alternative means of protecting personal data could suffice, - the AI practice shall be limited with respect to the unique characteristics needed. The frame includes only those bits of personal data that could avoid the absolute identity proof of the person concerned in the process of unique recognition and, at the same time, could be enough to verify a concerned personhood [3, p. 211]. The GDPR Article 88 (2) explicitly mandates Member States to incorporate adequate and precise measures into these ordinances to protect human dignity, legitimate interests, and necessity as well as Member States are entitled to establish specific requirements and more complex regulations regarding unique identification under Article 9 (4). It is especially needed when attention is also given to transparency of data processing, personal data transfers within the same group or group of companies, and workplace monitoring systems.

Biometric identification can be a convenient option in the workplace as it eliminates the need for employees to remember passwords or use other identification methods, such as access cards. This method also adds an extra layer of security by providing a unique identification method [9]. The question of whether less intrusive methods could meet privacy protection requirements needs to be clarified. For instance, using fingerprint access control at a gym may be disproportionate when weighed against the risks to the rights and freedoms of individuals. Similarly,

biometric identification in workplace access control must be analysed in terms of proportionality. While smart technology practice is typically justified on security grounds, more is needed to enhance security, as biometric data can also be collected without an employee's knowledge. It is, therefore, crucial to consider proportionality when determining the conditions for using biometric identification. This includes analysis of joint elements about (1) whether biometric identification is necessary to fulfil the current need, (2) whether it is an effective way to meet demand, and (3) whether there are potential adverse effects on the privacy protection of individuals. In the view of the research, if intelligent technology is employed, adequate security measures, such as determining retention times and else technical and organizational means of security shall be taken care of. Suppose the employer needs to use biometric data, such as a fingerprint, to provide access to a high-security risk area. In that case, the employer must store data as an encrypted code and ensure that the system holding the code is secure.

Access control is an everyday practice for biometric identification in a workplace; experience shows that unique recognition needs to replace access cards as the primary means of employee detection for controlling access to workplaces. Monitoring working hours using biometric data, such as with modern hour card systems, is like biometric identification for access control, as both identify a person upon entering a workplace. However, unlike access control, it is challenging to justify AI for monitoring working hours, as it has different security considerations. Privacy statement requirements may also limit the utilization of biometric systems. Additionally, integrating time attendance and access control systems can streamline operations and enhance security measures which can extend beyond traditional workstations, including laptops, desktops, tablets, and various applications.

Nowadays, employees can securely access work-related devices utilizing biometric authentication methods. For instance, Microsoft Windows Hello for Business offers facial recognition and fingerprint authentication, which is widely operated in companies operating on Microsoft Workstations. Also, a compelling legislative example is the authorisation of the French Data Protection Authority's (FDPA) in AU-027 – Deliberation n°074 on Unique Authorization for the use of fingerprinting in professional laptops stipulating that fingerprint templates must be stored exclusively on a limited number of professional laptops available to employees for work-related access. It is also required that fingerprint samples are only enrolled during enrolment. Furthermore, only one or more fingerprint templates, not an image or picture, can be saved, and the content cannot be read without the employee's knowledge. The templates must be encrypted using an algorithm that prevents reference to the sample, and data processing is limited to a user ID, password, and pattern. In deduction, AI methods for time attendance and access control systems are significantly enhance security measures in the workplace. However, it is crucial to implement proper steps to protect employees' data and maintain compliance with relevant regulations. The primary distinction between biometric identification and access control systems is that access control and time and attendance tend to be entirely «employer-controlled» since AI can be more fragmented when logging into workstations and applications. This is because the employer may only sometimes have complete control over whether an employee uses biometric identification, as noted by Neace [9, p. 74].

Furthermore, the choice between using biometric authentication or identification depends on the specific use case. Authentication is typically used when logging into workstations or systems through an AI. Generally, is assigned to a particular person, and authentication confirms a person's identity. In contrast, access control and time attendance systems can be based on either authentication or identification, depending on whether biometric identification is used alone or in combination with other identification methods. For instance, when the person is identified among all system users. However, if biometric identification is combined with another identification method, such as a pass card, settings can also operate based on authentication. In such scenario, the pass card identifies the person, followed by AI to confirm that the card holder is the rightful one.

When an employer processes an employee's data, it is essential to guarantee that the processing is legal, and the GDPR provides several conditions for this. GDPR Article 6 (1, b) states that the processing shall be performed under a contract, legal obligation, or consent. Hence, the processing can be permitted if it is legally required and there is, at the same time, the employee consents. Implementing smart technology may be necessary to fulfill the employment contract and to meet security needs. For example, employers should collect, and report data related to employee work performance, issue attendance records, and monitor working hours per statutory conditions. In some cases, there may be a legal obligation to use biometric data, such as fingerprint identification, to ensure the safety and security of individuals and property. However, employing AI must be justified and accompanied by strict safeguards to ensure legal processing. Implementing biometric identification can also be necessary to fulfill the employment contract, such as when assigning specific workstations to employees. However, using biometric data must be balanced against the employee's right to privacy and data protection.

According to the research, France, the first Member States country, in 2007, has already guided the use of AI in a workstation, expressing that it must be justified and combined with strict safeguards to protect the physical integrity of persons, goods, installations, or information. However, the research hypothesis argues that those criteria applied arbitrarily. The business may rely on a higher security interest to protect authorized persons who use unique characteristics. Those who are not authorized may not invoke the same security interest.

It is a legitimate aim to collect data for maintaining order and safety, and smart technology plays a crucial role in improving and reinforcing external borders. In fact, the EU has been developing large-scale IT systems for collecting and processing biometric data to enhance border security. The Commission Implementing Decision of 30 November 2018 delivers technical specifications regarding security features and standards. Prior to that, according to the European Data Protection Supervisor (EDPS) Opinion of 15 May 2014 on a notification for prior checking received from the Data Protection Officer of the European Parliament in Connection with the Biometric Verification Device Case, an employer's legitimate interest in ensuring security of its premises and information systems, enabling access to information, information systems, and managing office space, justifies the processing of personal data required for access control. However, the study contends that processing personal data is necessary for a company to carry out its tasks in various situations, even if a legal obligation, consent, or agreement cannot justify the processing. The EDPS did not explicitly refer to fundamental rights but rather to personal data protection legislation. Hence, the proportionality assessment is beneficial as per EDPS Guidelines on Assessing the Proportionality Measures that Limit the Fundamental Rights to Privacy and the Protection of Personal Data of 19 December 2019.

Furthermore, under GDPR Article 4 (11), consent must be a «voluntary, individualized, informed and unambiguous» expression of intent. In an employment relationship, consent is rarely considered appropriate as it may not be freely given, and the employee's interest must be deemed subordinate to the employer. The suitability of permission in the context of an employment relationship is the relevant exception to the GDPR Article 9 (2) for processing specific categories of personal data. Collection of a biometric identifier is challenging to see as a justifiable condition for concluding an employment contract because a biometric identifier is not necessary data for the employment contract as, for example, name and contact details. In the case of the unique identification practice, the legal basis for processing cannot become an implementation of the deal. On the other hand, AI practice could be based on the employer's statutory obligation where the legitimate interest of the employer and the restriction on its performance should be emphasised. Concerning biometric identification, the employer's legitimate interest remains the most appropriate legal basis for the proceedings if prior there has been a friendly instruction with an employee.

According to Article 6(1)(f) of the GDPR, the legitimate interest (basis) for processing personal data does not apply if an employee's data requires protection or if fundamental rights and freedoms outweigh the benefits of processing. Therefore, when using the legitimate interest as a legal basis for processing, a balancing test must be conducted to determine the controller's legitimate interests versus the data subject's fundamental rights and freedoms. In AI, this balancing test poses a significant challenge. It is crucial to weigh whether utilizing biometric identifiers not proportionally interferes with the rights and freedoms of the data subject. Although a legitimate interest may to be the most appropriate basis for processing biometric data in an employment relationship, the application of GDPR requires the applicability of exceptions strictly stipulated in Article 9 (2). As a result, a legitimate interest can ultimately only apply if one of the exceptions to the exceptions applies, which typically requires express consent from the data subject (a), or specific legislation in the employment context that permits processing (b). The research has found that if none of the exceptions outlined in Article 9(2) of the GDPR applicable, obtaining explicit consent under the conditions of a valid license is the only legal exception for biometric processing. However, when installing biometric systems in the workplace, avoidance of the infringing employee protection is crucial. For instance, access control to premises and areas requiring restricted access for security reasons should not compromise employee personal data under GDPR. Therefore, the principle of proportionality serves as a measure to ensure employee personal data protection while balancing the interests of all parties involved. Also, employers can leverage biometric applications to facilitate administrative tasks such as monitoring employee attendance and working hours or accessing services like meals. However, deploying a biometric system in such cases is typically done for all employees or third parties with permit, making it difficult to limit its use to only a limited number of data subjects. Thus, employers must ensure that the deployment of AI systems does not unduly compromise employee privacy.

The importance of providing an alternative identification method when assessing the valid nature of consent, particularly in employment, has been emphasized in recent rulings. For instance, the Swedish Authority

for Privacy Protection (Datainspektionen) permitted biometric identification for workplace access control and working time monitoring, subject to the employee's consent and the availability of an alternative, less invasive means of identification. Similarly, an airline practice there is a fingerprint-based passenger identification as an alternative identification means. However, in a recent Decision (Docket) of the Swedish Authority for Privacy Protection No DI-2019-2221 on Supervision under EU Data Protection Regulation 2016/679 regardless facial recognition for pupils' attendance control, it was deemed that the criteria for voluntary consent were not met, even though students had the option to opt-out and use traditional attendance methods. This was due to a significant mismatch between the controller and the data subject, making it difficult to consider the consent to be voluntary as guides the GDPR Recital 43. Although employees may also be disadvantaged in their relationship with their employer, the situation differs from that of young people to be under an authority's control. Therefore, the Swedish Authority for Privacy Protection's solution remains in question. In the view of the study, providing an alternative identification method is crucial in ensuring that consent is voluntary, especially in employment, where the power imbalance between employer and employee may affect the voluntariness of the approval. The study argues against drawing the determination that consent to process data using intelligent techniques should be mandatory in working life, even when alternative identification methods are available. The most common option for access control is the access card. However, if an employer seeks to improve the safety of its premises by utilizing two-step identification and wants to use biometric identification as an add-on to an access card (e.g., multimodal identification), the situation becomes more complicated. Nevertheless, guaranteeing sufficient safety with less privacy intervention is still achievable by using an access card and a code. Consequently, according to Article 4 (7) of the GDPR, the controller is the entity that determines the purposes for processing personal data. The French Data Protection Authority (FDPA) in Deliberation no° 2016-187 (AU-053) of 30 June 2016, relating to the single authorization for the implementation of devices whose purpose is to control access by biometric authentication to premises devices, and computer applications in the workplace, refers to the controllers as those who conservate templates in database. This regulative landscape means that the controller decides why and how the data is processed, including decisions about which employees are authorized, for instance, to collect data for specific purposes and by certain means. In the case of a workstation, for example, the employer defines that biometric data shall be collected to manage access to a workstation.

Sometimes, the situation can become complicated when the employer needs IT knowledge to manage workstations, such as in small companies. In such cases, the employee may be free to choose the method of logging in. However, the employer may still be considered a data controller even in this situation. This creates a problem because the employer determines that access must be managed but practically cannot govern the means to do so. To address this issue, the employer should take action, such as seeking expert advice or implementing appropriate policies and procedures. Unlike workstations, mobile devices are typically personal devices that are not always under the employer's control and may not require a code or biometric authentication to unlock. In addition, the employer may only be able to erase the device's memory if it is, for example, stolen. Although biometric data is processed when unlocking a mobile device, and it is unclear whether the employer is the controller. As per the FDPA Deliberation no° 2016-186 (AU-052) of 30 June 2016, relating to the single authorization for the implementation of devices whose purpose is to control access by biometric authentication to premises, devices, and computer applications in the workplace and guaranteeing control by the person concerned on their biometric template, the employer does not process biometric data. Therefore, a study suggests that the employer should not be considered a controller. This issue is significant for biometric data, because if the employers are not considered the controller, they are not responsible for ensuring the lawfulness of the processing of such data. In addition, the same technique includes BYOD (bring your device) principle, as per the EDPS Opinion on the Commission Proposal for a Regulation of the European Parliament and of the Council on a European Network of Employment Services, Workers' access to Mobility Services and the Further Integration of Labour Market of 3 April 2014, when employer can escape from the GDPR approach.

Therefore, assessment the employer's systems to which the staff's device can be logged «in» is important. The employer defines the purposes and means of processing. It is important to note that logging into the employer's systems is essentially separate from the authentication to unlock the device, which is not the case with logging into the device itself.

**Conclusions and Recommendations.** Consent is an unambiguous expression of desire, and a critical component of GDPR; it shall meet a voluntary criterion to be valid. However, in the context of an employment relationship, the condition of voluntary service can be particularly problematic, given the power imbalance between the employer and employee. Despite this, employers shall demonstrate that consent has been given voluntarily in

certain situations. Consent must be voluntary to apply for permission as a legal basis for unique identification under Article 6 or as an exception to Article 9 (2, b), which allows biometric identification in an employment relationship. Under GDPR Article 7 (1), the employer must be able to demonstrate that the data subject has given their consent. To guarantee that permission to operate intelligent processing is voluntary, employees shall have a option to refuse without penalty. In practice, if AI is used for login and access control purposes of workstations and systems, there must be an alternative to biometric identification. Otherwise, an employee must consent to log in or access the necessary techniques, which deems to be not valid.

For biometric data processing of workers, consent should not be used as a legal basis for proceedings. Instead, consent should only be considered when no other legal bases for unique recognition performance or exceptions are suitable. A case-by-case assessment is necessary to determine whether consent is appropriate as a legal basis for processing. Even when consent is deemed appropriate, it must be informed indication of the employee's «will». Instead, the data subject must consent in a way that indicates that they accept the proposed processing of their data. Merely abstaining from activities such as changing default settings cannot clearly indicate an employee's «will». Although the regulation does not impose a formal requirement for consent, it is crucial to ensure that it is evident that the data subject has agreed to the specific processing of their data. In recap, using consent as a basis for legitimizing smart technology in an employment relationship must be cautiously approached. Employers must ensure that employees have a genuine choice and provide clear and concise information about the scope of data processing. Under the GDPR Article 4(11), consent should be a statement or act that clearly expresses the data subject's «will» and should not be granted through silence.

To show compliance with the mentioned provision, explicit consent is required when processing specific personal data. While the criteria for a standard license have already become more stringent with the GDPR, additional conditions are necessary for an explicit permission. One way to ensure the exact nature of consent is to request the employee's signature for written consent, although other options exist. Electronic forms, emails, and electronic signatures can also provide explicit consent in the digital environment. Even the «yes» and «no» buttons on internet pages can be deemed explicit consent if the text indicates the approval being given. However, it is not ideal when regulation do not define explicit actions. Thus, it is essential to inform workers clearly about the type of consent requested and what they are consenting to. This emphasis on clear communication underscores the importance of ensuring that workers are fully informed when they agree. The employer must provide transparent and verifiable information to employees about processing personal data before seeking their consent. It is also essential to consider whether workers fully understand the implications and risks of biometric data processing when company, for example, changing the policy.

When logging into workstations or systems, it is crucial to consider whether consent can be given by changing settings. Consent must be voluntary, individualized, and unambiguous to guarantee the responsible AI use in the workstation. Cancelling consent should be as easy as giving it; if consent is given through an electronic interface, it should also be possible to withdraw it by the same understandable interface as also demonstrated in the GDPR Recital 32. To implement technical solutions for biometric identification, companies should ensure that withdrawing consent means a stop to process biometrics and removal of all links to a person's identity. Hence, companies should ensure that those conditions are met. Furthermore, employees shall receive sufficient information before consenting.

To ensure the responsible use of biometric data as a unique identifier, - companies must provide clear and easily accessible information about how this data used. While the GDPR does not mandate a format for providing this information, it must be communicated clearly and in understandable language. Additionally, workers should be informed if the biometric system creates an individual model or if the algorithm generates the same model for multiple systems. Consequently, employers need to confirm that the employee understands what they agree to, and to assess any potential negative consequences of processing biometric data in an employment relationship.

Another vital aspect to consider is the circumstances in which an employer can be deemed the controller of biometric data. This becomes particularly relevant when unique identification is not used in the employer's overarching governance systems, such as access control systems, but in employee-controlled devices, workstations, and mobile devices. In such cases, the employer may have some level of control over the workstations used by employees, but the obligations of a controller under GDPR may not necessarily apply. Furthermore, it raises questions about where the boundary between employment and personal life lies - while an employer may provide a mobile device, it is also often used for personal activities - blurring the lines between a tool for work and a personal device, making it challenging to define privacy and data protection responsibilities clearly.

In summary, the research outcome (1) shows that time-attendance detection of employees by artificial intelligent practice should be reviewed to assess the benefits and risks involved; (2) stresses the importance of providing guarantees to the employee regarding access to personal data without delay, as well as the need for employers to restrict access to the database by third parties; (3) recommends interdisciplinary research on utilizing biometric characteristics by innovative automated techniques, and (4) calls for regulations that provide transparent, purposeful, and comprehensible artificial intelligence practice for non-legal expert citizens, in particular, for employers and employees. Finally, (5) the research warns that an employer's neglect of organizational and technical backup procedures fails to assess risks fully and may result in insufficient protection of employee personal data.

## References

1. Bulgakova, D. (2021). *Application of the Principle of Proportionality on Biometric Data Processing in European Union Law*. University of International Business and Economics (UIBE), Law Faculty, Doctoral of Laws Degree Dissertation, 1-371 [in English].
2. Bulgakova, D. (2022). Case Study on the Fingerprint Processing in a Workplace under GDPR Article 9 (2, b). *Teisė*, *124*, 22-38. Retrieved from https://doi.org/10.15388/Teise.2022.124.2 [in English].
3. Bulgakova, D. (2022). The Protection of Commodified Data in E-Platforms. *Analytical and Comparative Jurisprudence,* 1 (2022), 208–212. Retrieved from https://doi.org/10.24144/2788-6018.2022.01.39 [in English].
4. Cefaliello, A. & Kullmann, M. (2022). Offering false security: How the draft artificial intelligence act undermines fundamental workers rights. *European Labour Law Journal*, *13* (4), 542–562. Retrieved from https://doi.org/10.1177/20319525221114474 [in English].
5. Warhurst, Ch, Mathieu, Ch. & Dwyer, R. E. (2022). *The Oxford handbook of job quality* (Chris Warhurst, Chris Mathieu, & Rachel E. Dwyer, Eds.). Oxford University Press [in English].
6. Georgieff, A. & Hyee, R. (2022). Artificial Intelligence and Employment: New Cross-Country Evidence. *Frontiers in Artificial Intelligence*, *5*, 832736–832736. Retrieved from https://doi.org/10.3389/frai.2022.832736 [in English].
7. Kassir, S., Baker, L., Dolphin, J. & Polli, F. (2023). Publisher Correction: AI for hiring in context: a perspective on overcoming the unique challenges of employment research to mitigate disparate impact. *Ai and Ethics (Online)*, *3*(1), 345–345. Retrieved from https://doi.org/10.1007/s43681-022-00225-w [in English].
8. Kuziemski, M. & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, *44*(6), 101976–101976. Retrieved from https://doi.org/10.1016/j.telpol.2020.101976 [in English].
9. Neace, G. (2019). Biometric privacy: Blending employment law with the growth of technology. *The John Marshall Law Review*, *53* (1), 73 [in English].
10. Qiu, H., Li, M., Bai, B., Wang, N. & Li, Y. (2022). The impact of AI-enabled service attributes on service hospitableness: the role of employee physical and psychological workload. *International Journal of Contemporary Hospitality Management*, *34*(4), 1374–1398. Retrieved from https://doi.org/10.1108/IJCHM-08-2021-0960 [in English].
11. Sowa, K., Przegalinska, A., & Ciechanowski, L. (2021). Cobots in knowledge work; Human -- AI collaboration in managerial professions. *Journal of Business Research*, *125*, 135. Retrieved from https://doi.org/10.1016/j.jbusres.2020.11.038 [in English].
12. Upchurch, M. (2018). Robots and AI at work: the prospects for singularity. *New Technology, Work, and Employment*, *33* (3), 205–218. Retrieved from https://doi.org/10.1111/ntwe.12124 [in English].
13. Weiss, D., Liu, S. X., Mieczkowski, H. & Hancock, J. T. (2022). Effects of Using Artificial Intelligence on Interpersonal Perceptions of Job Applicants. *Cyberpsychology, Behavior and Social Networking*, *25*(3), 163–168. Retrieved from https://doi.org/10.1089/cyber.2020.0863 [in English].

The article was submitted to the editorial office of the journal on 09.03.2023
Стаття надійшла до редакції 09.03.2023