Vilnius University Press

Contents lists available at Vilnius University Press

Teisė
2022, Vol. 124, pp. 22–38

ISSN 1392-1274 eISSN 2424-6050
DOI: https://doi.org/10.15388/Teise.2022.124.2

Case Study on the Fingerprint Processing in a Workplace under GDPR Article 9 (2, b)

Daria Bulgakova

ORCID https://orcid.org/0000-0002-8640-3622
Doctor of Laws
Ph.D. in International Law, Qualified Lawyer
Vilnius University, Faculty of Law
306 room (Dean's Office)
Saulėtekis av. 9 – I block, LT-10222 Vilnius, Lithuania
Phone: (+370 5) 236 61 85
E-mail: tf@tf.vu.lt
E-mail: dariabulgakova@yahoo.com

The protection of personal data is the most important legal standard for the use of biometric data. Fingerprints are personal biometric data in accordance with Article 9 (1) of the GDPR. It is also a category of personal data that needs to be processed specifically in order to ensure the right to the protection of personal data and to reduce the risk of its restriction. The problem discussed in this study is fingerprint processing in the workplace.
Keywords: Personal Data Protection, Unique Identification, Biometric Data, Automotive Processing, Finger Recognition.

Teismų praktikos tyrimas dėl pirštų atspaudų apdorojimo darbo vietoje pagal BDAR 9 straipsnio 2 dalies b punktą

Asmens duomenų apsauga yra svarbiausias biometrinių duomenų naudojimo teisinis standartas. Pirštų atspaudai yra asmens biometriniai duomenys pagal BDAR 9 straipsnio 1 dalį. Tai taip pat yra ir asmens duomenų, kuriuos reikia apdoroti siekiant užtikrinti teisę į asmens duomenų apsaugą ir sumažinti šios teisės pažeidimo riziką, kategorija. Įsigilinus į šį tyrimą, galima teigti, jog pirštų antspaudų apdorojimo darbo vietoje reiškinys yra problemiškas.
Pagrindiniai žodžiai: asmens duomenų apsauga, unikalus identifikavimas, biometriniai duomenys, automatinis apdorojimas, pirštų atpažinimas.

Introduction

The General Data Protection Regulation (hereinafter referred to as 'GDPR') (Regulation (EU) 2016/679...)) has a direct implementation in the Member States of the European Union. Member States should assume that any national measures that could apply throughout the EU contrary to the Lisbon Treaties will be demarcated contrary to EU law (ECJ, Case 94/77...). Repetition of the text of EU regulations in national law is prohibited unless such repetitions are strictly necessary to ensure consistency (ECJ, Case 94/77...). However, in some cases, implementation measures are required by EU regulations themselves to ensure uniform application across the Union (ECJ, Case C-34/73..., 98, para. 10). In implementing the norms of European acts in the legislation of the Member States, an important issue is how provisions of the national laws will diverge. GDPR contains over forty rules

Received: 18/05/2022. **Accepted:** 22/06/2022

and can be deciphered by the Member States. Reproduction of the text of GDPR verbatim in special national laws must be exclusive, justified, and cannot be exploited for additional conditions or interpretations. It affects the practice of GDPR and even leaves the state a relatively narrow framework for adopting additional provisions. Member States have to take the necessary steps to reconcile legislation by repealing or amending provisions of GDPR. Requirements of the GDPR can be instantly summoned by citizens, legal entities, government agencies, and other organizations falling under its scope. In this regard, EU institutions shall implement a framework for interpreting the provisions of data protection law in the Union uniformly. Also, it allows the Member States to clarify or supplementary adjust data protection rules in exact areas: public and municipal sector; employment and social security; preventive and professional medicine; public interest; scientific, historical research, or statistic (Jori, 2019, p. 528).

Thus, stating the situation in 2018, from over 27 countries Member States of the EU only five – Bulgaria, Greece, Malta, Romania, Portugal – did not immediately react to the reformation (McKenzie, 2018, p. 37; See more in http://europa.eu/rapid/press-release_MEMO-19-462_en.htm). EC warned those countries with a call to comply with Digital Single Market legislation (Communication from the Commission EU law...). In that way, Member States must reform the national personal data protection law until May 6, 2022. Otherwise, infringement cases may be directed to the Court of Justice of the European Union. It plays an essential role in the compliant application of personal data protection law in the EU, justifying national norms. Furthermore, the EU Commission submits an assessment report to the European Parliament and the Council of Europe every four years about GDPR compliance across the union.

Regardless of the above, uniform and consistent regulation in the union largely depends on the actions of the Member States to adopt national laws in accord with EU law. For the implementation provisions concerning the processing of special categories of personal data, Member States should consider the principle of proportionality, especially when it comes to biometric data processing. The application should be under the particular condition of assessing the necessity to process biometrics (Steps of the assessment outlined in: European data protection supervisor. Quick-Guide to...). Member States are allowed to introduce conditions and limitations in the means of the studied article (GDPR, Article 9 (4)). The position of national legislation recommended having a course on further restrictions to process biometric data with respect for human dignity, moreover, with a forbidden dimension of human body elements (De High, 2018, p. 1286). That is because of the risk of trade and business financial gain of human characteristics (De High, 2018, p. 1286). It became indispensable, particularly from the moment of introduction Digital Market Strategy and digitalization course (European Commission. Press release on March 9 of 2021...).

The general rule about biometric data processing states that usage of biometric technology must be only a method for the person's identification when other techniques do not work, and the unique recognition corresponds to its necessity. A company shall deliver alternative methods if a person does not want to provide physical, physiological, or behavioral characteristics. The Parliamentary Assembly adopted a resolution about the elaboration of Member States for the habit application of the legal definition of biometric, based on the reformation policy of the data protection field. The approach goes against everyday body partial scans spreading the principle of proportionality[1], and its harmonization

[1] Council of Europe Parliamentary Assembly. Resolution 1797 (2011) On the need for a global consideration of the human rights implication of biometrics of March 11, 2011 states the application of proportionality by heeding steps: ,limiting evaluation, processing, and storage of apparent necessity, significantly when the gain in security outweighs a possible interference with human rights and less intrusive techniques does not suffice; providing individuals who are unable or unwilling to provide biometric data with alternative methods of identification and verification'.

(TFEU, Art. 288). National law can specify possible restrictions and limitations for regulating biometric data processing by clauses use (Chakarova, 2019). For example, a clause in Article 9 (4) GDPR enables the Member States to introduce additional conditions for special categories of personal data (CJEU Case C-673/17..., and the Opinion of the AG Szpunar, March 21, 2019). In the view of the study, a clause does not request harmonization measures but its practical implementation at the national level (Miscenic, Hoffmann, 2020), and sincere cooperation (TEU, Art 4 (3)). Upon legal nature, GDPR's opening clauses are classified as obligatory. In that vision, norms concerning biometric data processing give the Member States some way of defining additional legal grounds permitting the processing of such a distinct category and separately stipulate data sort out.

The Netherlands, in response to GDPR, adopted the Implementation Act (hereinafter referred to as the 'UAVG') (Uitvoeringswet Algemene Verordening...) launched on May 25, 2018. The former Act, known as Wet Bescherming Persoonsgegevens (hereinafter referred to as the 'Wbp'), has ceased to apply (Wet bescherming persoonsgegevens..., 2012). Wbp did not contain specific rules for biometrics; therefore, it is challenged that UAVG, on the one hand, provides specific national derogation and, on the other, similarity to the provision of Article 9 (2) GDPR. Thus, the inclusion of biometric data processing and an extension of the types of personal data became crucial. The UAVG has prohibited to process biometrics and issued national affairs for this matter (UAVG, Articles 22, 23). It is allowed only if there is a necessity for authentication and security purposes (UAVG, Article 29), likewise, biometric access systems to computers and buildings.

On May 12, 2017, the German Bundesrat approved the Federal Data Protection Act on the Adaptation and Implementation of GDPR provisions (Datenschutz-Anpassungs-und-Umsetzungsgesetz...)[2]. published further on July 5, 2018. It came into force, like GDPR, on May 25, 2018. Former Data Protection Act (Bundesdatenschutzgesetz, 2003) in the time of the provisions of Directive 95/46/EC ceased to apply. Thus, Germany is the first European country to adopt its national legislation immediately. Germany subjected biometric data processing to several different legal requirements. The first, if necessary, biometric data is permitted for the processing to achieve public interest. Secondly, the processing is allowed without a person's consent for scientific, historical, and statistical research purposes. Third, public and private bodies may process biometrics in preventative or occupational medicine, in employment, contract, and if the processing is subject to secrecy. Thus, the controller's interests substantially outweigh the data subject. Germany also provides a safeguarded technique when data could be processed and stored on an identity card at the request of the card applicant.

Italy is distinguished from all EU countries by the existence of the Personal Data Protection Code.[3] Provisions for the Adaptation of the National Legislation (Decreto legislativo of Aug. 10, 2018...) amended the former Code. Italy introduced the following limitations when biometric data must obey specific safeguards: encryption, pseudonymization, minimization, and selective access. Also, under the Italian Data Protection Authority (hereinafter referred to as the 'IDPA'), biometric data processing is safeguarded for healthcare organizations to diagnose patients and medical prescriptions. The novel is prohibition of the dissemination of biometric data.

[2] Article 1, Sections 2–7 amend and change other related laws such as the Protection of the Constitution Act, the MAD Act, the Security Audit Act, and others.

[3] Personal data protection code Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons regarding the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC.

1. Problem

Case 1. December 4, 2019. The Decision of Dutch Data Protection Authority 'Boetebesluit vingerafdrukken personeel'

On July 5, 2018, the Dutch Data Protection Authority (hereinafter referred to as the 'DDPA') launched an investigation about fingerprint processing in the workplace. The exploration took place based on the information that the company (hereinafter referred to as the 'Company 1') invited employees to collect physiological characteristics (DDPA Report 'Examine staff..., 2019).

Based on the testimonies, the purpose of mentioned processing is a unique identification of employees due to the need to fix the time of duties performed in the office. A biometric scanning kit became an avoidance measure of the excessive absence of employees from time to time during working hours. Risk mitigation is justified because workers must accomplish tasks while staying in the workplace (DDPA Decision 'Fine decision..., 2019, at 2)). Company 1 updated its policy to control employees' arrival and departure times through computerized records of fingerprint processing (DDPA Decision 'Fine decision..., 2019, at 2)). Therefore, in the view of Company 1, a unique recognition system is a definitive and accurate method to control workers' onsite duties. Company 1 calculated the amount of factual working time and consequently guaranteed pay salary appropriately to exact hours wage. Moreover, the equipment is beneficial because it levels out the purchase cost, loss, and damage of formerly used personal identification cards. Among other things, fingerprint processing is a solution for unwanted third parties' entry and exit problems (DDPA Decision 'Fine decision..., 2019, at 2)). Thus, by replacing an outdated system, unique identification is expected to eliminate security risks hereafter.

From organizational and technical points of view, employees should leave at least two finger footprints in biometric embedded installment. Once characteristics were brooked, templates with the finger's unique data were preserved as a text file. As a result, Company 1 has collected physiological characteristics from the structural information of employees' bodies and achieved a unique identification purpose in the workplace. Biometric records were enclosed upon the termination of employment. Within the employment relationships, times-off and days-off duties, fingerprint patterns were saved and remain locked in the company's biometric base.

The biometric embedded application for fingerprint processing has been in operation since early 2017. The first fingerprint processing took place on January 23, 2017. Nevertheless, employment contracts had no stipulations about fingerprint processing for unique identification purposes. In July 2017, Company 1 warned employees about the necessity and purpose of fingerprint processing through the supplied handbook (DDPA Decision 'Fine decision..., 2019, at 2)). Several employees indicated that fingerprint processing was mandatory for payroll applications. Two employees confirm about given verbal consent. Other employees refused to provide finger's physiological characteristics, and the following talk with the director about this negative feedback took place (DDPA Decision 'Fine decision..., 2019, at 2)). On November 8, 2018, fingerprint processing was running at last. On March 18, 2019, some of the employee's biometric data were still active in the database (DDPA Decision 'Fine decision..., 2019, at 2)). After April 16, 2019, Company 1 ceased to store the fingerprint templates and text files of formerly employed employees.[4]

[4] It is proposed to distinguish the period of fingerprint processing before GDPR's effectiveness and after that. It was explored that from January 23, 2017, until May 25, 2018, there were 250 employees whose fingerprints were processed. Starting on November 8, 2018, the total amount of processed fingerprint templates was 337.

Case 2. June 4, 2020. LArbG Berlin-Brandenburg 10th Chamber Decision[5]

On June 4, 2020, the appeal court, LArbG Berlin-Brandenburg, completed a hearing of the case about the biometric time recording of an employee based on the plaintiff's lawsuit against the company (hereinafter referred to as the 'Company 2'). Plaintiff has been a radiologist since June 1, 2007, and employed as a medical and technical radiology assistant.

From August 1, 2018, the defendant used the ZEUS Firma I of GmbH, IT 8200 FP platform for the timesheet record of personnel's daily hours and ensured proper accounting of working hours. It enabled a weekly duty to be assembled (LArbG Berlin-Brandenburg 10..., 2020, at para 4). A new stated technique is fingerprint-based biometric identification. On July 27, 2018, all employees were briefed about the invention because previously, employees had to record working hours on the duty roster manually. Company 2 noted: 'From August 1, 2018, only working hours being determined through emergence timekeeping system are applied. Hours recorded on the duty roster are no longer recognized' (ArbG Berlin 29, Kammer Decision..., p. 2 para 5). Nevertheless, a plaintiff used a manual method for working hours records. The plaintiff refused to use the disputed time recording system, notably by failing to give consent. Therefore, in August and September of 2018, the plaintiff retained the former record system without biometric data processing operation. On October 5, 2018, the defendant issued a warning.[6] On March 26, 2019, the warning was regurgitated.[7] The plaintiff also requested the defendant to remove those written warnings from the personal labor file.

The practice of unique finger identification has increased the development of new technologies and its embrace by the company (ArbG Berlin 29. Kammer Decision..., p. 4 para 19). Company 2 considers all the rebutted warnings lawful because biometric data processing refers to the GDPR Article 9 (2, b). The plaintiff's consent to apply the biometric installment for the time record is not mandatory. Biometric innovation has been familiarized to all employees, and each employee shall follow policy. Besides, an outdated manual timekeeping system posed a risk of unauthorized access to employee information. Alternative recording methods such as ID numbers and electronic chip cards have been halted. As a result, the wrongful calculation of actual time spent cannot subsequently be verified and recorded without errors. Thus, employees' ID card systems are inaccurate because staff can falsely pass cards to colleagues. The defendant argued about the experience of its parent company. For example, various digital time recording systems under chip cards or transponders had negative experiences because they could change registered data without much effort. Some employees pass chip cards or employee identification numbers to colleagues several times and, as a result, illicitly encumbered the time into the data system (ArbG Berlin 29. Kammer Decision, p. 4 para 19). Also, when the chipboard is forgotten or lost, Company 2 cannot document working hours accurately. Company 2 cannot always check the actual attendance and declares that biometric technologies are shielded from counterfeiting

[5] Ruling the ArbG Berlin 29 Kammer Decision of October 16, 2019, – the company representative, on November 18, 2019, filed an appeal to LArbG Berlin-Brandenburg 10th Chamber.

[6] Para 13 of the Kammer Decision of LArbG Berlin-Brandenburg states: ‚We request you perform duties using the ZEUS logging system through fingerprint with immediate scanner effect. Suppose you continue to falter in following our instructions. In that case, we will impose further employment law measures, up to job termination'.

[7] Para 15–16 of the Kammer Decision of LArbG Berlin-Brandenburg states: ‚Despite our written request and warning dated October 5, 2018, unfortunately, we had to reveal that you are not using the ZEUS recording system. A time-clock device is essential for managing hourly and holiday accounts with your duty schedule. We are, therefore, forced to warn once again and for the last time. You have to carry out duties by using the ZEUS timetable. Please carry out duties using the ZEUS with the appropriate fingerprint scanner. If you fail to follow our instructions, we will impose additional measures under the German labor laws. Immediate termination is also possible if the violation continues'.

(LArbG Berlin-Brandenburg 10. Kammer Decision..., 2020, page 7, paras 40–41). Thus, the biometric system is instantly conjoined to the automotive calculation of completed duties.

It is stated that a machine does not pose any risks for the employees because staff only need to provide some parts of physiological finger characteristics in contrast to a whole finger's footprint.[8] Besides, the processing is managed uniformly through the human resources department.[9] Furthermore, the plaintiff's assignments are performed at high-risk; thus, fingerprint processing is necessary not only for accurate time recording but also to eliminate chains of infection (LArbG Berlin-Brandenburg 10. Kammer Decision..., 2020, page 8, paras 43). In this regard, Company 2 retrieved the plaintiff's health data through fingerprint processing (LArbG Berlin-Brandenburg 10. Kammer Decision..., 2020, page 7–8, paras 42). In that way, in the view of Company 2, the interests of both are harmonized.

Case 3. January 14, 2021. The Decision of Italian Data Protection Authority about 'Ordinanza ingiunzione nei confronti di Azienda sanitaria provinciale di Enna'

In November 2019, on premises of the Provincial Health Institution Enna (hereinafter to as ‚Enna') remain known about application of a biometric technique to ensure more excellent technical reliability in verifying the identity of each discourages phenomena of absenteeism (Resolution of April 4, 2019 – Regulation no. 1/2019...). It has resulted in the initiation of an investigation against Enna by IDPA.

The company provides its services in 21 municipalities with over 2000 employees. The administration has introduced the system of biometric identity verification for the decentralized control and triggered in light of Law no. 56/2019 (IDPA, Ordinanza ingiunzione..., 2021, Article 2, Page 2). It confirmed the practice of finger processing in four clinics and territorial wards allocated in municipalities. Biometric data processing was performed for different employees due to 24 hours tasks and led to considerable complexity of the duties management.

An Enna argued that there are no critical violations of norms because the installment uses ‚…[s] oftware that can capture data and store it in encrypted form on a secure device. All employees have been equipped with the information under Article 13 of the GDPR. Besides, the software offers a data deletion phase' (IDPA, Ordinanza ingiunzione..., 2021). Assuming biometric data processing involves the detection of the fingerprint transformed into an encrypted string, stored in turn of the badge. 'The system compares strings of fingers stored in the badge locally and only within the time necessary for verification and when a comparison is coincident. A processed computed string is automatically deleted; therefore, biometric is no longer stored, and only the serial number of the employee, time, and date of attendance has been seated.' (IDPA, Ordinanza ingiunzione..., 2021) The time detection is performed by contextual use of the badge and placing the employee's finger on the device. Besides, Enna did impact assessment, taking the registration, enrollment, acquisition, and recognition phases for the attendance records under the contractual relationship with its employees (IDPA, Ordinanza ingiunzione..., 2021, Article 3 (3.1); General prescriptive provision on biometric..., 2014). Enna has warned the staff and informed the trade union, issuing detailed notes containing generic references to ensure correct and transparent processing (GDPR, Article 13).

[8] On December 17, 2019, have defended the substantiated position about an urgent need to use the processing of fingerprints; otherwise, there may be an abuse of the record time.

[9] The company 2 has adopted special security measures under Section 22 of the Federal Data Protection Act in the interests of its employees.

2. Problem Assessment

GDPR covers biometric data to be regulated and obtained through specific technical processes. It also includes physiological characteristics of an individual, which allow to make a unique identification or confirm the unique identification of that individual (GDPR, Article 4 (11)). Article 9 (1) of the GDPR expressly regulates the prohibition of biometric data processing. The processing of personal data consists of ‚any operation or set of operations, carried out with or without the aid of automated processes and applied to personal data or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, comparison or interconnection, limitation, cancellation or destruction' (GDPR, Article 4 (2)). Biometric data processing is not prohibited if one of the grounds for derogation applies (GDPR, Article 9 (2)). Based on the circumstances of the studied cases, the research took exemption 'b' prolonged in Article 9 (2) of the GDPR. The mentioned exception is vigorous because it makes questionable biometric data processing in the workplace.

The companies consider it legitimate to set up the processing of fingerprints that records working hours. For further discussion, the study counts the principle of proportionality because the processing of fingerprint data is a subject matter of proportionality application.[10] The application proposed is to be made according to the criteria of the mentioned principle. Among them is a balance of interests and aims pursued. The claim in three scenarios involved the interest of a company to control the time-attendance of employees by fingerprint processing, and the welfare of employees is to protect their biometric data. Consequently, it is necessary to establish whether employees' biometric data processing is proportional to the need for timekeeping to exercise rights and fulfill obligations. The interests of the employee and company must be proportionate to each other. On the counterweight, these interests could be legally shunned when employees' biometric data is processed to disclose or avoid criminal offenses (Directive (EU) 2016/680 of the European Parliament...). The legal basis of the processing must, among other things, pursue an objective for public interest and be proportionate to the legitimate aim pursued.[11] Although the employee's unique identity is affirmed at the access gates, a study believes this particular treatment is under justification because the processing is carried out directly and personally by the interested party in privileges.[12] In this regard, whether the aim in studied cases – unique identification is justified – must be confident.

Employers' general commitments rule out reliable and accessible systems for calculating hours worked per day by every staff member. Therefore, companies indicate that such processing is necessary. In the view of the study, the need for the attendance sheet, security, and work management are not pertinent because employees for access control should gain credentials by enrolling biometric features into a fingerprint system. The DDPA states that fingerprint processing for the prevention the time and attendance regime is neither necessary nor proportionate (DDPA Report 'Examine staff..., 2019). In

[10] Recommendation CM/REC (2015) of the Committee of Ministers to Member States on the processing of personal data in the context of employment, paragraph 18 (1) 'Biometric data': 'The processing of biometric data should be based on scientifically recognized methods and should be subject to the requirements of strict security and proportionality' (1224 meeting, April 1, 2015).

[11] GDPR, Article 6 (3, b); Recommendation on the protection of personal data used for employment purposes, the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data [ETS No. 108], paragraph 18 'Biometric data': 'The access to such data shall be subject to requirements of security and proportionality' (October 30, 2012).

[12] GDPR, Articles 5, 6, 9; (IDPA, Ordinanza ingiunzione..., 2021, para 3.3 states about the absence of a legal basis for processing of biometric data to detect attendance.

the view of the study, companies in three studied cases are correctly pointing out that the employer should not tolerate incorrect entry of working hours to a certain extent. However, due to the explicit prohibition of biometrics processing, companies must be guided by GDPR Article 9 (1) (2). Also, proportionality is applied to the risk level and type of risk for the person whose biometric data is processed. Company 2 guaranteed fingerprint processing control, demanding uniform time tracking using a fingerprint scanner uniformly through the human resources department.[13] However, on the other hand, Company 2 disclosed the plaintiff's health data due to the risk of infection associated with a specific employee position in a radiological office. After all, he works in sizeable radiological equipment and has access to saline solutions. Therefore, in the view of Company 2, an accurate recording is necessary to eliminate the chains of infection and protect other employees. In the opinion of the study, health data is included in the special categories of Article 9 (1) of the GDPR and is not subject to processing or disclosure. The system's installation would not replace a broader framework of initiatives for the imposition of disciplinary sanctions and sanctioning noncompliance with worktime. Thus, the degree of data protection in the company is low. In this respect, there is interference and risk posed to privacy.

The person's interests are at stake with the company when biometric data processing occurs. There must be appropriate guarantees for the fundamental right to personal biometric data protection. The employer must determine the scope of preventive measures based on an overall risk assessment. The following argument is proposed. A study predefines a synthetic computer description of the obtained biometric characteristic which only extracts the elements from the biometric sample. In all cases, the biometric apparatus requires the registration phase through a precise reading of the employees' fingerprint to create a biometric model in Case 3 securely stored in the badge given to the person concerned. In the subsequent phases of biometric recognition of the interested party, an Enna verifies the identity through biometrics in the badge, and this obtained model is presented for the time detection. Generally, if the comparison operation is successful, it can ascertain the interested party's identity. The function is possible because the employees' registration number is transmitted to the attendance management system, and also data about the date and time of being in a workplace. Based on the view of the study, Enna guarantees the right to data protection because biometric conservation is applicable in badges with intelligent functionality that the administration entrusts to each interested party (employees), that in response, is the exclusive holder. There must be a high level of individual control over personal biometric data. It demonstrates taken procedures, both technical and organizational, that, among other things, complied with the minimization of the objected data (GDPR, Articles 5 (1, c), 24, 25). However, in any case, the preliminary verification of when the conditions of lawfulness are met in processing of employees' biometric data is open. Hence, a study thinks that the more such measures are implemented, the more likely the fingerprint processing will pass the sense of proportionality measurement.

In the view of the study, given the employer–employee relationship, explicit consent cannot be disowned. In this circumstance, parties are obliged to elaborate the definiteness and purpose of the machining carefully under a collective agreement. Therefore, the exception under GDPR Article 9 (2) (a) is not taken in this circumstance. According to cases' facts, companies had no documentation of proof of will for fingerprint processing. In the first two cases, some employees were confronted with this operation. Likewise, the DDPA investigation revealed refusal, as several employees said that fin-

[13] In Case 2 company used terminal „IT 8200 FP" with the model of the time-registration system „ZEUS" from a company I. GmbH. A system for reading an ID card and transponders is that such an installation allows identifying a person without processing the plaintiff's fingerprint. Also, the electronic system „ZEUS" of I. GmbH saves the corresponding timesheet, as far as even without the biometric data of the claimant, so that system produces alternative methods of E-registration and not only based on the fingerprint database.

gerprint scans were mandatory (DDPA Report 'Examine staff..., 2019, at 3). Thus, Company 2 did not take the necessary organizational measures to pursue a collective agreement. Introspection presumes that reconciliation is not depend on the parties' status. For instance, an employer is a person who willy-nilly is engaged in the relationship involved. Nevertheless that the employer can keep a record of all employees concerned up to date, and these records are made available to the competent authorities (ECJ, Case C 55/18..., para 34), in Case 2, the warnings dated October 5, 2018, and March 26, 2019, have no legal basis and must be removed from the employee's file (LArbG Berlin-Brandenburg 10..., 2020, page 14, para 81). In Case 1, several employees indicated that when they refused to have their fingerprints scanned, a conversation with the director followed. Significantly applying the principle of proportionality, there is an imbalance of interests. Given the dependency on the employer–employee relationship, employees could feel it is an obligation instead of ask to register fingerprints. In the view of the study, the collective agreement is valid when each of the employees states a will in a written declaration. Thus, unique identification in Cases 1 and 2 is not legitimate because a collective agreement is not delivered. That established breach of GDPR Article 9 (2, b). No derogation can be earned in any case, even with the consent of the employee concerned (ECJ, Case C 55/18..., para 39). In Case 3, none of the disagreement has been found. Moreover, Enna indicated employees' unique identification by applying Article 2 of Italian law No. 56 of June 19, 2019, affected from November 4, 2019. Moreover, according to documental findings, it is declaring that Enna has been deploying biometric systems consistent with the opinion of a draft Decree issued by the President of the Council of Ministers concerning problems. In the view of the study, those facts comply with the GDPR Article 9 (2, b) criteria about a collective agreement and Member State law authorization.

Turning to the security assertion, the study proposes to examine whether the employer's security interests are legitimate. The company vindicates a high-security gain that may exceed the employee's interest in particular facts. Employers envisage biometric access control to increase access security. Employers are interested in reserving access to their premises, such as factories, offices, or special facilities, and adequate access to certain facilities only for employees or contractors. In the view of the study, the employer protects designated infrastructures rather than shielding workers. An alternative method, such as the use and verification of an employee's or contractor's number at the entrance to the premises, would, in principle, be sufficient to satisfy security interests. The research thinks it is relevant for real security needs especially when a company must monitor the identity and the permit is only to a limited number of specifically authorized persons that could have access to certain facilities and places and solely confirmed in an enhanced manner. Pursuant to case studies, employers have implemented a system that can measure the daily working hours of each employee. The employer must have an objective, reliable and accessible design to measure the daily working time of each employee. In Case 2, the company stated that the primary purpose of functioning the ZEUS time roster and the IT 8200 FP terminal is to prevent wrongful tab a working time. The modern alternative technologies are very diverse for limiting the maximum working hours and observation of daily rest periods. It can be a system for recording working hours, records in paper form, computer programs, and electronic displays for recording working hours (LArbG Berlin-Brandenburg 10..., 2020, page 10, para 60). The card systems that make it possible to hand over cards to colleagues avoiding to be too late and leaving early are likely a violation of the list of duties and have to be deemed a breach of labor law and cannot be an argument for using Article 9 (2, b) as an exception from Article 9 (1) of GDPR. Therefore, the reasoning of data transmission to colleagues and manipulation of the time – pretending as being present, but factually not – is outside the GDPR and not an unprecedented circumstance that can be an exception. Besides, it can also be viewed as fraudulent worktime and thus constitute a criminal

offense. Nevertheless, the processor must assess the fundamental right to personal data protection through a delicate balance that considers the interests of both. The study assumes it in the first two cases. In Case 3, the security reasons explained due to the 'considerable complexity in the management of employees' (IDPA, Ordinanza ingiunzione..., 2021, Article 3 (3.3)) with amount of over 2000, and the vastness of the territorial area.

In the view of the study, compared to Case 1 and Case 2, Case 3 demonstrates that a biometric setting is proportional to the actual circumstances of processing of employees' fingerprints. Enna proves the processing protection in an encrypted way. It is not permitted to record encrypted data in a manner that is incomprehensible to the person who is privy to understanding it. In the view of the article, a centralized repository of biometric data is an adequate security measure where the storage of samples should be sidestepped. Data storage should be carried out without explicit reference to the individual or other types of personal data, e.g., name. But Company 1 and Company 2 demonstrate the opposite. At this point, the study deems to provide additional protection, such as using a pseudo-name or code-name. The study argues that, in any case, biometric data must be handled under human control, considering human dignity (Explanatory memorandum to Recommendation Committee of Ministers No. R. (89) 2..., provision 43, 45) and privacy (Explanatory memorandum to Recommendation Committee of Ministers No. R. (89) 2..., provision 70). Regardless of that, the Enna shows compliant operational biometric usage because the new detection system of attendance comes into operation using the biometric sensor keeping data storage only on the personal card, and held only by the employee. In other words, data has been saved only on portable devices equipped with cryptography capabilities and used in badges entrusted to each staff (IDPA, Ordinanza ingiunzione..., 2021, Article 3(3.2)).

Moreover, based on GDPR Article 5 (1, a), a study thinks the processing appears to have been carried out in violation of transparency; as indicated above, case facts do not fully represent the carried-out processing. Thus, any company has not demonstrated that employees have been sufficiently informed about fingerprinting.

As a result, according to Case 1, on December 4, 2019, DDPA imposed a fine of 725,000 EUR under violation of Article 9 (2, b) from May 25, 2018, to April 16, 2019.[14] In Case 2, the Berlin-Brandenburg Regional Court held that an employer could not rely on Article 9 (2, b) to install a time-tracking system that uses employees' fingerprints. The Appeal court states that utilizing a biometric system in a workplace is not proportional. GDPR Article 9 (1) is understood in the context of banning to process biometrics for neither time management nor control of attendance in the workplace.[15] In Case 3, the IDPA imposed a EUR 30.000 fine against Enna – a local public health body – using employees' biometric attendance detection system.

Thus, specific legislation for the use of biometric applications is limited. In this context, the possible distorted use of the tools for detecting the everyday presence in a workplace and the decisions of employees assessed to the relative treatment are nonproportionate (Provision no. 357 of September 15, 2016...). However, the research disagrees with the fine in Case 3 and states Enna's compliance that led to an independent research position. Given the extent of the number of employees affected – 2000 in service – a biometric detection system is necessary case-to-case and could not be generalized as illegality in the Enna casefor most of the working time control in medical or surgical practice. Also,

[14] DDPA Decision is also according to the GDPR Article 58 (2) and Article 83(5). Those provisions are set out in the Netherlands' UAVG Article 14 (3). Moreover, the Company 1 is officially enlisted in the Commercial Register of the Chamber of Commerce and Industry, whose number is also concealed.

[15] The appeal is admissible but not substantiated. The Regional Labour Court – LArbG Berlin-Brandenburg 10. Kammer - followed the Decision of Berlin Labour Court – ArbG Berlin 29 Kammer.

taking into account specific characteristics of the biometric system, the last does not memorize biometric data, resides on the badge, and is read-only at the time of stamping. The registration phase 'enrollment' is carried out using a personal computer and an optical sensor connected through an interface entirely inside the device. The fingerprint detected on the registration site is immediately transformed by the sensor into a string of encrypted bits and sent to the personal computer that records it in a template of the unique identification medium (smart card with a microchip). Thus, when the employee puts a finger for the processing, an image is stored only for the time necessary for processing, obtaining the representative finger string (the template) from the characteristics of the imprint. it is impossible to get the fingerprint image starting from the bits string (template) stored on the smartcard.[16] Moreover, the described system for the detection of biometric data, in its inactive state, falls within the scope of application of the regulations set forth regarding the protection of personal data, to the extent that the company intends to acquire the information in the enrollment phase deducible from the employees' fingerprints – by storing them on the badge entrusted to the staff. A worker has an opportunity to press 'agree' to enter; at this stage, there is no memorization and even less transmission of images of the footprint or the template, and apart from temporary local storage as well as concerned device is for the sole purpose of recognition when at the same time the biometric data remain confined to the sensor and deleted at the end of the process. Thus, Enna safeguarded the processing and mitigated the risk of privacy interference (European data protection supervisor guidelines..., December 19, 2019).

Conclusion

The processing of personal data relating to the detection of attendance and working hours is attributable to the purposes pursued by entities under a regulatory framework that provides specific obligations to control consequent responsibilities of the competent functions of administrations within the scope of institutional tasks assigned to them by labor law promoting disciplinary actions. Regarding the use of biometric technologies to detect attendance, it is noted that the legitimate purpose ascertained for compliance with working hours utilizing objective and automated forms of controls (and in some cases to guarantee exceptional levels of security) must, in any case, be carried out in full compliance with the regulation on the protection of personal data. Because the right to personal data protection is not absolute, a study concerns compliance with the principles of necessity and proportionality. The research requires that other physical and logistic safety systems, devices, and measures are considered to ensure a timely and reliable verification for workplace control without biometric data processing. Biometric data are personal data directly, univocally, and in a tendential way stable over time, connected to the individual and denote the profound relationship between the person's body, behavior, and identity – and its use for the specific purpose of recording attendance in service, which the company intends to pursue, is not proportional to the needs of the company under data protection legislation. The employer is always required to seek the less invasive means by choosing, if possible, a nonbiometric procedure.

Regarding the protection of personal data, it is noted that detailed elements provided by the data controller concerning repeated and concrete episodes of violation of office duties by employees and the well-founded fear of the perpetration of abuses, compliance of the working hours by the employees, together with the possible benefits deriving to the community from the effective unique detection of presence in service, – examine cases peculiar. For the same assessment, those aspects are relevant to

[16] Two encryption levels protect the series of bits (template): the 1st level is inherent in the (proprietary) transformation logic. The 2nd level uses the authentication key of the smart card itself.

guiding the company‘s choice towards the described attendance detection system and deemed to the toponymy and the extension of the area because it does not allow easy control of the presence of the workers and observance of working hours. In this context, we must consider proportionality concerning the purposes pursued and the need for the continuous availability of biometrics for service reasons to move frequently from one department to another. The conduct of companies intends to prevent the situation when an unfaithful employee goes to mark in place of a set of colluding colleagues, absent at work. The companies had documented reasons for ineffective alternative automated tools and the difficulties encountered in carrying out the correct execution of the services to employees. In these cases, the daily verification of the presence of the personnel assigned for the sanctioning regime is not compliant in Cases 1 and 2.

When an employer processes an employee‘s biometrics, it becomes the legal basis for the processing based on the conditions of the performance of the contract (GDPR, Article 6 (1, b)), the legal obligation to process biometrics and the agreement implication to make the processing valid. However, a company must process personal data to carry out its tasks in various situations, even if a legal obligation, agreement cannot justify the processing. In the light of the circumstances described in Case 3 and the system configuration of methods of using biometric data processing, in the view of the study, Enna complied with the exception provided under GDPR Article 9 (2, b). The prime necessity to manage a large number of facilitated employees in the institution is justified and combined under technological and organizational safeguards for employees and met processing for a vital interest of adequate healthcare that exceeds Enna’s interests and aims to protect workers‘ physical integrity by giving back processed finger ID saved on the smart-chip card under self-control.

The study also encounters the employer‘s legitimate interest in ensuring the security of its premises and information systems, enabling access to information, information systems, and managing the office space (European Data Protection Supervisor, Opinion..., May 15, 2014). This employer is justified for the processing measure since personal data is required for access control (European Data Protection Supervisor, Opinion..., May 15, 2014). As regards the condition for processing – the consent (GDPR, Article 6 (1, a)) has been rarely considered appropriate in an employment relationship; therefore, the employee‘s interest is subordinate to the employer. Public or private owners could start processing except for their close and stable relationship with the individual and identity (IDPA, Ordinanza ingiunzione..., 2021, Article 3, at 3.3). Therefore, the legal basis for processing cannot be under the agreement in all cases, as collecting a biometric identifier is contested to see a justifiable condition for an employment contract (European Data Protection Supervisor, Opinion..., April 7, 2008). However, processing can comply with the employer‘s statutory obligation for biometric identification (European Data Protection Supervisor, Opinion..., April 7, 2008). In this regard, the employer‘s legitimate interest remains the most appropriate legal basis for the proceedings concerning biometric identification. The legitimate interest provided does not apply if ‚the employee‘s interests require personal data protection or fundamental rights and freedoms override such benefits‘. (GDPR, Article 6 (1) (f)) Therefore, legitimate interest as a legal basis for processing requires a so-called balancing test, which weighs the legitimate interests of the controller (employer) and the fundamental rights and freedoms of the data subject (employee) (European data protection supervisor guidelines..., December 19, 2019). The proportionality test is the stumbling block; it is necessary to weigh whether the processing interferes disproportionately with the rights and freedoms for the employee’s benefit. A balance of interests involved could have been the most appropriate treatment for using biometric identifiers in the employment relationship. Therefore, a legitimate interest as a basis for treatment will ultimately necessarily apply, especially where processing is not expressly permitted by specific legislation like in studied cases.

Companies referred to particular security need permitting on that way biometric data processing. This criterion, however, is applied in a rather willful way. Companies may rely on this higher security interest to protect persons under received authorization. In the view of the research, the DPA of a particular country may grant approval for using biometric characteristics, particularly fingerprints, to secure access to places. For example, the Dutch DPA states that it is legitimate to collect data to maintain order and safety.[17] However, this general rule, in principle, requires specific legislation on biometric identification in an employment relationship under the GDPR exception of Article 9 (2, b). It is the known fact that GDPR allows the Member States to adopt additional biometric rules in the context of employment.[18] Some of the provisions, such as Article 88 of the GDPR, are no exception for the further broader interpretation. Hence, the scope of a specific regulation adopted in Member States countries is limited (LArbG Berlin-Brandenburg 10..., 2020, page 11, para 62). The criterion for processing biometric data in the employment context is not different from the general rule. Thus, no deviation or modification is permitted in the national law of Member States. The derogation is not applicable because there is no particular legislation on biometric identification in employment activities in studied countries. [19]

In the study‘s view, installing biometric systems in a workplace should not abuse employee data protection. Since the deployment of a biometric system is usually carried out for all employees, it cannot limit its use to only a limited number of data subjects. Employers cannot impose restrictions on worker rights.[20] Moreover, the EU law does not require employers to create a system to measure the length of the working day worked by each employee every day (ECJ, Case C 55/18...). Therefore, there is no legal basis in the means of GDPR Article 9 (2, b) for employees‘ biometric data in the workplace.

[17] The process of determining a person‘s identity through a database search is practiced against multiple sets of data (one-to-many check). A measurable unique, physical characteristic or personal behavioral trait is used to recognize the identity or verify the claimed identity of a person. Technology can play an integral role in improving and reinforcing external borders. Over the past years, the EU has been developing large-scale IT systems for collecting and processing; See Brussels, 7774 final Commission implementing decision of 30.11.2018 laying down the technical specifications regarding the security features and biometrics standards.

[18] GDPR, Article 9 (2, b) (4), Article 88. For example, the German legislator has implemented these norms of GDPR in section 26 of the BDSG.

[19] The situation is not the same in EU countries. The need for biometric identification by employers has been identified in France by the National Data Protection Regulation; the reform of the data protection legislation included a provision on the possibility for employers to use biometric identification following the Model Rules of the French Data Protection Commissioner, CNIL, https://www.cnil.fr/fr/biometrie-sur-le-lieu-de-travail-la-cnil-lance-une-consultation-publique-sur-le-futur-reglement-type (last visited August 1, 2021); Data Protection Act amended by the Law No. 2018-493 of June 20, 2018, and by the Decree No. 2018-687 of August 1, 2018. France counts as a pioneered Member State in the problematic field. France already had a specific regulation for biometric data processing; therefore, this issue was not innovative for legislators. Thus, under the GDPR Article 9 (4), the French legislator introduces additional conditions for biometric data processing. Firstly, shall drive the processing on behalf of the state. Secondly, biometrics may be processed if necessary to verify a person‘s identity. The processing has to be also authorized by the Decree Council of State issued after a substantiated opinion of the French Data Protection Authority. The processing due to the state‘s security, defense, or public safety shall be permitted. Also, the authority may prescribe additional technical, organizational, and other measures to ensure legal guarantees for individuals. Therefore, the experience of France is suggested for further research.

[20] ECJ, Cases Pfeiffer and Others, C-397/01 to C-403/01, EU:C:2004:584, para 82, 5 October 2004; Fuß, C-429/09, EU:C:2010:717, para 80, 25 November 2010; Max-Planck-Gesellschaft zur Förderung der Wissenschaften, C-684/16, EU:C:2018:874, para 41 (6 November 2018).

Bibliography

Legal acts

Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (2018). *Council of Europe*, *128th Session of the Committee of Ministers,* CM/Inf(2018)15-final.

Resolution on the Need for a Global Consideration of the Human Rights Implication of Biometrics (2011). *Council of Europe Parliamentary Assembly*, 1797.

Recommendation on the Protection of Personal Data used for Employment Purposes (2012). *The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS No. 108.

Explanatory Memorandum to Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (2015). *Council of Europe*, *Committee of Ministers, 1224th meeting of the Ministers' Deputies,* CM (2015) 32.

Charter of Fundamental Rights of the European Union (2009). *Official Journal of the European Union*, 2016, C 202/389 (2016/C 202/2).

European Parliament and the Council 2016, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing directive 95/46/EC (General data protection regulation). *Official Journal of the European Union*, L 119/1.

European Parliament and the Council 2016, Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *Official Journal of the European Union*, L 119/89.

European Parliament and the Council 2017, Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final – 2017/03.

Communication from the Commission EU law: Better results through better application 2017/C 18/02 (2017). *Official Journal of the European Union,* C 18/10.

Data Protection Authorities 2016, Room document for the 38th International Conference of data protection and privacy commissioners, artificial intelligence, robotics, privacy and data protection.

The Future of Privacy Forum and Anonymity 2020, Report on the Practical Cases of the Processing Personal Data on the Basis of Legitimate Interests under the GDPR 41.

International Conference of Data Protection & Privacy Commissioners (ICDPP) 2018, Declaration on Ethics and Data Protection in Artificial Intelligence.

European Group on Ethics in Science and New Technologies 2018, Statement on Artificial Intelligence, Robotics and Autonomous Systems.

European Data Protection Board 2014, Regulatory recommendations of EU expert group 2 for privacy, data protection, and cybersecurity in the smart grid environment on data protection impact assessment template for smart grid and smart metering systems.

European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice 2018, Shared Biometric Matching Service (BMS) Feasibility study – final report.

European Data Protection Supervisor 2008, Opinion on a notification for Prior Checking received from the Data Protection Officer of European Anti-Fraud Office on Identity and Access Control System, Case 2007-0635.

European Data Protection Supervisor 2014, Preliminary opinion on privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the digital economy.

European Data Protection Supervisor 2014, Opinion on the Commission proposal for a regulation of the European Parliament and the Council on a European network of employment services, workers' access to mobility services and the further integration of labour market.

European Data Protection Supervisor 2014, Opinion on a notification for prior checking received from the Data Protection Officer of the European Parliament in connection with the 'Biometric verification device' case.

European Data Protection Supervisor 2015, Opinion 7/2015 meeting the challenges of big data, a call for transparency, user control, data protection by design and accountability.

European Data Protection Supervisor 2016, Opinion 9/2016 on personal information management systems towards more user empowerment in managing and processing personal data.

European Data Protection Supervisor 2016, Background paper for consultation, developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rigths.

European Data Protection Supervisor 2017, Assessing the necessity of measures that limit the fundamental rigths to the protection of personal data: a toolkit.

European Data Protection Supervisor 2019, Guidelines on assessing the proportionality measures that limit the fundamental rigths to privacy and the protection of personal data.

European Data Protection Supervisor and Agencia Espanola protection datos 2019, Joint paper introduction to the hash function as a personal data pseudonymisation technique.

European Data Protection Supervisor and Agencia Espanola protection datos 2020, Joint paper on 14 misunderstanding with regard to biometric identification and authentication.

European Data Protection Supervisor 2020, Explanatory paper on monitoring and enforcing compliance with regulation (EU) 2018/172.

European Data Protection Supervisor 2020, Quick-Guide to necessity and proportionality.

Wet bescherming persoonsgegevens (Wbp) (2012). *Official Gazette of the Kingdom of the Netherlands,* 90 Bulletin of Acts and Decrees.

Resolution of April 4, 2019 - Regulation no. 1/2019 concerning internal procedures with external relevance, 106 Gazzetta ufficiale della Republica Italiana.

Decisions of the Data Protection Authorities in The Netherlands and Italy

The Dutch Data Protection Authority. Decision of December 4, 2019 (Published on April 30, 2020) 'Boetebesluit vingerafdrukken personeel' ('Fine decision on fingerprint staff (Non-official translation in English)) [online]. Available at: boetebesluit_vingerafdrukken_personeel.pdf (autoriteitpersoonsgegevens.nl) [Assessed 1 April 2022].

The Dutch Data Protection Authority. Report of December 4, 2019 'Ondeerzoek vingerafdrukken personeel' ('Examine staff fingerprints' (Non-official translation in English)) [online]. Available at: onderzoek_vingerafdrukken_personeel.pdf (autoriteitpersoonsgegevens.nl) [Assessed 1 April 2022].

Italian Data Protection Authority. Injunction of January 14, 2021 'Ordinanza ingiunzione nei confronti di Azienda sanitaria provinciale di Enna - 14 gennaio 2021' ('An Injunction against the Provincial Health Authority of Enna' (Non-official translation in English)) [9542071] No 16 [online]. Available at: Ordinanza ingiunzione nei confronti di Azienda sanitaria provinciale di... - Garante Privacy [Assessed 1 April 2022].

Special literature

Caruana, N. (2018). Employment Law General Data Protection Regulation. *GHSL online law journal*, 1.

Chakarova, K. (2019). General Data Protection Regulation: Challenges Posed by the Opening Clauses and Conflict of Laws Issues. *Stanford-Vienna European Union Law*, 41 (11).

De Hingh, A. (2018). Some Reflections on Dignity as an Alternative Legal Concept. *Data Protection Regulation. German Law Journal*, 19 (5), 1269–1290. https://doi.org/10.1017/S2071832200023038

Giacomo, F. (2019). The User-Centric and Tailor-Made Approach of the GDPR through the Principles It Lays down. *Italian law journal,* 5 (2), 631–672.

Gonzalez, F. (2014). Fighting for Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection. *Birkbeck law review,* 2 (2), 263–277.

Hoeren, T., & Kolany-Raiser, B. (Eds.) (2018). *Big Data in Context*. SpringerBriefs in Law, https://doi.org/10.1007/978-3-319-62461-7_10

Hutton, C. (2019). Linkability, Personhood and State Modernity: Understanding the Affordances of Personal Identity across Different Legal Regimes. *Law & Literature*, 31 (2), 239–257. https://doi.org/10.1080/1535685X.2018.1530840

Kindt, E.J. (2013). *Strengths and Weaknesses of the Proportionality Principle for Biometric Applications*. Privacy and Data Protection Issues of Biometric Applications. Law, Governance and Technology Series, vol 12. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-7522-0_6

Lambert, P. (2020). *Understanding the New European Data Protection Rules*. Auerbach Publications, CRC Press.

Leibenger, D. *et al.* (2016). Privacy Challenges in the Quantified Self Movements – An EU Perspective. *Proceedings on Privacy Enhancing Technologies,* 2016 (4), 315–334. https://doi.org/10.1515/popets-2016-0042

Lorenzmeier, S. (2016). *European law — Quickly Captured (5th ed.)*, Springer Berlin Heidelberg.

MacCarthy, M. (2020). Enhanced Privacy Duties for Dominant Technology Companies. *Rutgers computer & technology law journal (2021),* 47(1). https://dx.doi.org/10.2139/ssrn.3656664

McKenzie, B. (2018). GDPR National Legislation Survey, 37. gdpr_national_legislation_survey.pdf (bakermckenzie.com)

Miscenic, E., & Hoffmann, A. (2020). The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR). 4 *EU and Comparative Law Issues and Challenges Series,* 54, 44–61. https://doi.org/10.25234/eclic/11895

Monajemi, M. (2018). Privacy regulation in the age of biometrics that deal with a new world order of information. *University of Miami international & comparative law review,* 25(2), 371–408.

Nguyen, F. (2018). The Standard for Biometric Data Protection. *Journal of law & cyber warfare,* 7 (1), 61–84.

Ronald, L., Van Brakel, R. E., Gutwirth, S., & De Hert, P. (Eds.) (2017). *Data Protection and Privacy: The Age of Intelligent Machines.* Oxford: Hart Publishing.

Sprokkereef, A. (2008). *Data Protection and the use of Biometric Data in the EU*. Fischer-Hübner, S., Duquenoy, P., Zuccato, A., Martucci, L. (Eds.) (2007). The Future of Identity in the Information Society. Privacy and Identity. IFIP — The International Federation for Information Processing, vol 262. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-79026-8_19

Suder, S., Erikson, M. (2021). *Microchipping Employees: Unlawful Monitoring Practice or a New Trend in the Workplace?*. Ebers, M., Cantero Gamito, M. (eds) Algorithmic Governance and Governance of Algorithms. Data Science, Machine Intelligence, and Law, vol 1. Springer, Cham. https://doi.org/10.1007/978-3-030-50559-2_4

Tamo-Larrieux, A. (2018). *Desighing for privacy and its legal framework.* Springer: Cham. https://doi.org/10.1007/978-3-319-98624-1

Jori, A. (2019). Hungary: Introduction to the GDPR Application and a Brief History of Data Protection. *European data protection law review. GDPR Implementation Series, 5 (4), 528*-532. https://doi.org/10.21552/edpl/2019/4/11

Electronic publications

European Commission. Press release on March 9 of 2021 at Brussels. *Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030* [online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983 [Assessed 1 July 2021].

Uitvoeringswet Algemene Verordening Gegevensbescherming (in Dutch) [online]. Available at: https://wetten.overheid.nl/BWBR0040940/2019-02-19 [Assessed 1 April 2022].

Datenschutz-Anpassungs-und-Umsetzungsgesetz (in German) EU - DSAnpUG-EU, Federal Law [online]. Available at: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1616466981499 [Assessed 1 July 2021].

Personal data protection code Law No 160 of December 27, 2019 [online]. Available at: https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3 [Assessed 1 July 2021].

Decreto legislativo of Aug. 10, 2018, n. 101. Gazzetta official della Republica Italiana (September 4, 2018) [online]. Available at: https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg [Assessed 1 July 2021].

General prescriptive provision on biometric, at '6.1', '6.2', '6.3' of attachment A to the condition of the Guarantor of November 12, 2014, n. 513 [online]. Available at: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/3556992 [Assessed 1 July 2021].

Court practice

LArbG Berlin-Brandenburg 10 Kammer Decision of 4 June 2020, ECLI:DE: LAGBEBB:2020:0604.10SA2130.19.00.

ArbG Berlin 29 Kammer Decision of 16 October 2019, ECLI:DE: ARBGBE:2019:1016.29CA5451.19.00.

Requirement to set up a system enabling the duration of time worked each day by each worker to be measured [CJEU], No. C 55/18, [14.05.2019]. ECLI:EU:C:2019:402.

Fratelli Zerbone Snc v Amministrazione delle finanze dello Stato; Reference for a preliminary ruling: Tribunale civile e penale di Genova – Italy [CJEU], No. 94/77, [31.01.1978]. ECLI:EU:C: 1978:17.

Fratelli Variola S.p.A. v Amministrazione italiana delle Finanze. Reference for a preliminary ruling: Tribunale civile e penale di Trieste – Italy [CJEU], No. C-34/73, [10.10.1973]. ECLI:EU:C:1973:101.

Case Study on the Fingerprint Processing in a Workplace under GDPR Article 9 (2, b)

Daria Bulgakova
(Vilnius University)

S u m m a r y

Protection of a person‘s data is a paramount legal standard for biometric usage. The fingerprint is personal biometric data within GDPR Article 9 (1). It is also a particular category of personal data that requires specific processing to ensure the right to personal data protection and minimize the risk of its restriction. The research interest leads to the problem of fingerprint processing in a workplace through the case study. The goal is molded to provide comparative research about the implication of the GDPR Article 9 (1) (2, b) by the Member States of the European Union in the Netherlands (2019), Germany (2020), Italy (2021). The case study is limited to the discussion about the processing of finger characteristics of employees in a workplace for the time-attendance detection. The European Union law requires employers to establish an objective, reliable and accessible system to measure the length of the working day each employee works each day (ECJ, Case C 55/18..., para 60), nevertheless, it is not a way forward for the GDPR Article 9 (2, b) application.

Teismų praktikos tyrimas dėl pirštų atspaudų apdorojimo darbo vietoje pagal BDAR 9 straipsnio 2 dalies b punktą

Daria Bulgakova
(Vilniaus universitetas)

S a n t r a u k a

Asmens duomenų apsauga yra svarbiausias teisinis biometrinių duomenų naudojimo kriterijus. Vadovaujantis BDAR 9 straipsnio 1 dalimi, pirštų atspaudai yra asmens biometrinis duomuo. Tai taip pat yra ir asmens duomenų, kuriuos reikia apdoroti siekiant užtikrinti teisę į asmens duomenų apsaugą ir sumažinti šios teisės pažeidimo riziką, kategorija. Atliktas mokslinis tyrimas atskleidžia, kad pirštų atspaudų tvarkymo darbo vietoje problema itin išaiškėja atliekant teismų praktikos analizę. Šio rašto darbo tikslas, pasinaudojant lyginamuoju metodu, pateikti tyrimą dėl BDAR 9 straipsnio 1 dalies bei 2 dalies b punkto taikymo šiose Europos Sąjungos valstybėse narėse: Nyderlanduose (2019 m.), Vokietijoje (2020 m.), Italijoje (2021 m.). Teismų praktikos tyrimas atliekamas tik dėl darbuotojų pirštų charakteristikų apdorojimo darbo vietoje, siekiant užfiksuoti darbo laiką. Pagal Europos Sąjungos teisę reikalaujama, kad darbdaviai sukurtų objektyvią, patikimą ir prieinamą sistemą, kuria remiantis būtų matuojamas kiekvieno darbuotojo darbo laikas (ETT, byla C 55/18, 60 punktas), tačiau tai nėra tinkamiausias būdas pritaikyti BDAR 9 straipsnio 2 dalies b punktą praktikoje.

Daria Bulgakova, Doctor of Laws, Ph.D. in International Law, Qualified Lawyer, Vilnius University, Faculty of Law

Daria Bulgakova, teisės mokslų daktarė, mokslų daktarė tarptautinės teisės studijose, kvalifikuota teisininkė, Vilniaus universiteto Teisės fakultetas