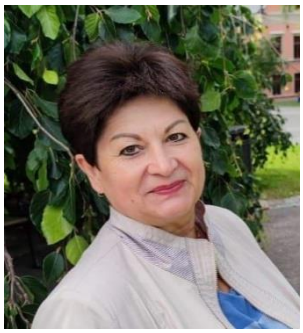

УДК: 341.1/.8
ORCID id 0000-0002-8640-3622
DOI https://doi.org/10.32703/2663-6352/2023-1-13-184-203
Daria Bulgakova
Postdoctoral Researcher in Technology Law
National Yang Ming Chiao Tung University,
School of Law, Taipei, Taiwan.
PhD in International Law, Lawyer,
Kryvyi Rih, Ukraine

ORCID id 0009-0009-6463-5228
Valentyna Bulgakova
Historian, Pedagogue-Methodist,
Supervisor of Scientific Manuscripts on History,
Sociology and Law in Dnipropetrovsk Oblast',
Gymnasium No. 91, Kryvyi Rih, Ukraine

BIOMETRIC DATA PROCESSING OF EMPLOYEES UNDER FRENCH LAW

Анотація. *Право Европейьского Союзу, а саме Загальне Регулювання Захисту Даних відоме як GDPR, забороняє унікальну ідентифікацію людини. Однак GDPR визначає умови виняткiв як у статті 9 (2, b), що дозволяє обробку даних працівників на робочому місці, надаючи державам-членам згідно статті 9 (4) пріоритет у визначенні уточнень у національному законодавстві. На думку авторів дослідження, обробка біометричних даних працівників, в принципі, вимагає спеціального законодавства у сфері трудових відносин. У Франції ж запроваджено Закон № 2018-493 від 20 червня 2018 року та Délibération № 2019-001 від 10 січня 2019 року. Оскільки біометричні характеристики включені до спеціальної категорії персональних даних, це викликає необхідність у подальшому роз'ясненні щодо засад використання біометричних систем на робочому місці шляхом спрямування уваги на побудову правових шляхів для їх особливого захисту. У зв'язку з цим автори статті досліджують законодавчу базу Франції в рамках захисту даних біометрії працівників та надають правову оцінку відповідаючи на наступне питання. Як роботодавці можуть запроваджувати та практикувати обробку біометричних даних на робочому місці згідно законодавству Франції і як при цьому дотримуватись вимог GDPR? Дослідження показало, що встановлення біометричних систем на робочому місці не повинно негативно відображатися на реалізації фундаментальних прав працівників захисту даних і гарантування приватності даних. Це означає, що контроль доступу до приміщень і зон з обмеженим доступом з міркувань безпеки не повинен перешкоджати забезпеченню гарантій для працівників відповідно до GDPR. На сьогодні в Франції дозволена обробка відбитків пальців для управління часом, та полегшення адміністративного навантаження як то при моніторингу робочого часу та встановлення факту відвідуваності працівників робочого місця або покращення умов отримання послуг, таких як харчування, у той же час аналіз вказує на необхідність оцінки ризиків та визначення критеріїв відповідності. Для цього дослідження пропонує застосовувати*

принцип пропорційності, що дозволяє не лише захистити персональні біометричні дані працівників, а й узгоджує інтереси сторін. Однак, оскільки застосування біометричної системи зазвичай здійснюється для всіх працівників або й навіть відвідувачів, тому її використання не може бути обмежене лише певною кількістю суб'єктів. В силу цього, роботодавцям пропонується слідувати критеріям оцінки відповідності Французьким правилам обробки біометричних даних на робочому місці та дотримання вимог GDPR, серед яких визначення необхідності у такому нововведенні, наявності правової підстави, явної згоди працівника на цільову унікальну ідентифікацію, надання роботодавцем пропозиції щодо альтернативних варіантів розпізнавання особи, та дотримання фундаментальних прав та свобод, зокрема приватності даних, захисту даних, повага до гідності та свободи у визначенні та виборі, а також впровадження організаційних та технічних заходів безпеки.

Ключові слова: *унікальна ідентифікація людини, GDPR, розпізнавання особи на робочому місці, технології, що підвищують конфіденційність, право на захист даних.*

Annotation. *The General Data Protection Regulation of the European Union, known as GDPR, prohibits unique human identification but provides exemption conditions for specific circumstances, such as employment, in Article 9, paragraph 2 (b). Member-States are also given priority to specify national legislation indications under paragraph 4. However, biometric data processing under this exemption in an employment relationship requires specific legislation, as demonstrated in French Law No. 2018-493 of 20 June 2018 and Délibération n° 2019-001 of 10 January 2019. This poses a challenge for employers, as biometric data is classified as personal data and requires further clarification on its use in the workplace. A manuscript aims to investigate French law on data protection regarding biometrics and assist employers in complying with GDPR. The research evaluates possible solutions after considering criteria in a workplace. It concludes that installing biometric systems should not compromise employee data protection and privacy. While the French approach to fingerprint processing for time management is functional, a risk assessment is necessary to protect employee biometric data and balance parties' interests. The manuscript recommends that employers shall levy the necessity of a valid legal basis, obtain explicit consent for a limited purpose, consider alternatives, respect fundamental rights, and implement appropriate measures to process biometric data in the workplace and comply with GDPR. While deploying a biometric system is usually for all employees, its use should not be limited to a few data subjects and, therefore, shall value overall company policy.*

Keywords: *unique human identification, GDPR, recognition in a workplace, privacy-enhanced technology, right to data protection.*

1. Introduction to the European Union Agenda

Big data offers significant benefits to individuals and society, including in areas such as health, scientific research, the environment, and other species. Scholar Minaj stresses the importance of acting with urgency in response to the integration of data processing into various legal and social norms around the world [13]. Despite the increasing prominence of these issues in the legal agenda, there still needs to be more consideration of the impact of these developments on people's rights and freedoms. Under the study of

Brumnik, the relevance of data protection depends on the extent to which it is needed [2]. The problem also appoints a scholar Mistale, especially about the legal uncertainty of how to guard the realization of a specific right to personal data protection [17]. In that respect, Article 41.2 of Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data - a predecessor to the current GDPR - established a supervisory authority to protect individuals' data. This authority, independent from any other public body, is responsible for overseeing data protection and privacy issues in the EU and for ensuring that the processing of personal data was carried out per the regulation's provisions prior to the introduction of 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 General Data Protection Regulation (GDPR), and therefore was replaced by the European Data Protection Board (EDPB) under the GDPR.

A scholar Sprokkereef [15], contends that the most commonly employed non-technical perspective to regulate the processing of biometric data is a legal-normative approach that actively was employed for the European Union (EU) data protection legal reform beginning in January 2012 with the adoption of a reform package based on the Communication about new general data protection regulations and data protection in the area of law enforcement, aims to strengthen and modernize the regulatory framework. A novel model of proportionality assessment, as highlighted in the Norwegian Data Protection Authority's Report on big data-privacy principles under pressure (2013), became an essential aspect of this reform effort. European data protection law provides robust protection for an individual's fundamental right to personal data protection, including the right to protection of biometric data processing. The key matter is not whether to apply proportionality to biometric systems within the context of big data but instead how to apply it effectively in the unique and ever-changing environment of digital data under the example of the French experience, regardless of unique identification in a workplace. This requires ongoing study and evaluation to stay current with the latest developments in the field. A scholar Lubin [12], refers to the international biometric standards that define biometric data processing as a comparison of supplied data with extant templates in a database to verify uniqueness and, if applicable, identify the individual in question.

In response to these challenges and risks, the European Data Protection Supervisor (EDPS) has emphasized the need for more effective protection of biometric data in the context of big data in a message of ‘Shaping a Safer Digital Future: A New Strategy for a New Decade’ published on 30 June 2020. Prior to that, the EDPS suggests that a proportionality assessment of data processing should include four key elements. Firstly, organizations must be transparent about how they process the data. Secondly, individuals must have control over their biometric data and how it is processed. Thirdly, businesses should design user-friendly data protection products and services. Fourthly, the law should hold businesses accountable for their actions. The EDPS emphasized the importance of transparency and accountability in their Opinion 7/2015, ‘Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability,’ of 19 November 2015.

According to the research view, the EU Digital Single Market can only adopt data-driven technologies and business models from other parts of the world and shall also evaluate the impact on people's unique characteristics, which can be exploited for profit. This demands a careful examination of unique characteristics. The GDPR Article 4 classifies biometric data into two legal categories. A scholar Worku [18] raises the interpretation and delivers highlights that the first category pertains to information related to physical characteristics, such as facial features, fingerprints, and other physiological features of an individual, and the second category pertains to information related to human behavior, which includes any unique behavioral characteristics that can be used to identify a particular person. Biometric technology should not be exploited to violate an individual's rights or to promote innovation at the expense of fundamental human rights. Given the manuscript hypothesis, companies must take the necessary steps to ensure that biometric data is proportional to the intended purpose and does not result in unintended consequences that may infringe on individual rights. Respectively, the EDPS embraces guarantees for the right to data protection that is constituted under the Charter of Fundamental Rights of the European Union (CFREU) Article 8 and Treaty on the Functioning of the EU Article 16 and confirms the devotion of compliance in its Opinion 9/2016 of 20 October 2016 on personal information management systems towards more user empowerment in managing and processing data. As Brkan [1] notices, the Charter of Fundamental Rights of the EU is a powerful significant legal tool for defending biometric data protection within the execution of the right to personal data protection.

Biometric characteristics are unique identifiers that pose social and security risks with the widespread use of biometric systems. GDPR has significantly changed the way biometric data is fettered. Biometric data processing is generally prohibited, except in cases that fall under one of the exceptions outlined in the GDPR Article 9 paragraph 2. Nevertheless, according to GDPR Article 9, paragraph 4, Member States may maintain or introduce other conditions, including limitations on the processing of biometric data, as France accomplished for the unique identification purpose in the workplace. France's experience is noteworthy because it was one of the EU's Member States that acknowledged the market for special biometric data protection. Furthermore, on the other hand, it permits unique identification in its national law concerning biometric data processing of employees. As noted by scholar Bulgakova [5], the main rule for biometric data processing is that it should only be used for identification when other methods fail and are necessary. Companies must provide alternative methods if a person does not want to provide their physical, physiological, or behavioral characteristics. In this regard, the research seeks to find out the France regulation on the use of biometric technology for access control to premises, equipment, or work applications experienced in a workplace and propose recommendations for further countries where such processing is still prohibited.

2. The French Law No. 2018-493 of 20 June 2018 and Délibération n° 2019-001 of 10 January 2019 on Exception Conditions from Ban to Process Biometrics

The exponential growth of biometric data presents serious concerns regarding unique identification and automated processing, particularly as large digital datasets become increasingly common in business, government, and other large organizations that rely on computer algorithms. Any business that deals with large

amounts of biometric data must ensure that its processing practices are proportional and appropriate. Authentic human characteristics in automated processing are legally safeguarded under the right to data protection. The French Act No. 78-17 of 6 January 1978, which has been in effect for over forty years with various modifications and additions, has been updated by the French government to align with GDPR without being repealed. The updates were adopted using an accelerated procedure to meet the GDPR's deadlines. Law No. 2018-493 of 20 June 2018 on protecting personal data amended the 1978 Act to take advantage of the derogation provided for in the GDPR Article 9 (4) and implement it into French law. Therefore, Law No. 2018-493 is being enforced in stages, with the amendments to the 1978 Act, and took effect on 1 June 2019.

The GDPR Article 54 mandates each Member-State to establish a supervisory authority, which is considered mandatory by legal experts. The activities of national supervisory authorities are streamlined by introducing legal mechanisms outlined in Section 1 of Chapter VII of the GDPR, titled 'Cooperation and Consistency.' This notice is part of a more considerable effort to establish a unified system of competent authorities across the EU, which requires the cooperation of European data controllers and, in some instances, controllers representing third countries. When carrying out their duties of control and supervision, both EU and Member-State authorized bodies primarily utilize imperative methods of influence, including recommendations, positive prescriptions, and opinions.

On 12 December 2018, Order No. 2018-1125 was disseminated to reorganize the French Data Protection Authority (FDPA). Following this order, the FDPA was reformed and renamed on 1 June 2019. Given that, after conducting a public consultation, **National Commission on Informatics and Liberty/**Commission nationale de l'informatique et des libertés (CNIL) has adopted the biometric regulation for the unique identification workplace', which outlines the obligations of employers who wish to use biometric devices for access control to spaces, applications, and work tools. Thus, on 28 March 2019 entry into force, CNIL Délibération n° 2019-001 of 10 January 2019 on standard (model) regulations for the implementation of devices for the purpose of entrance control by biometric authentication and is accompanied by practical guidance for companies on how to comply with these requirements.

This set of standards is the first standardized regulation that lays down legally binding rules applicable to data controllers who are subjects of French Law. It is particularly relevant for those who use biometric systems to control access to premises, devices, and workstation applications. The set prescribes specific requirements for processing information systems or applications used in business tasks entrusted to data subjects such as employees, agents, interns, and contractors by public and private employers. CNIL issued this document to comply with the obligation laid down in GDPR and to provide appropriate safeguards in respect of the fundamental rights and interests of biometric data subjects as, for example, under Article 1 of the Délibération n° 2019-001, data controllers should be demanded to conduct a data protection impact assessment. Regardless, businesses and organizations that process biometric data are obligated to comply with the standard regulations outlined by CNIL. This model applies to any use of biometric data by employers for workers, both in the public and private sectors.

While novel business models may utilize biometric technology to collect, process, combine, and reuse human characteristics, a clear principle of proportionality must be thoroughly considered to ensure compliance.

In addition to the principle of proportionality, modern principles such as accountability, transparency, limitation safeguards, and protection by design and default are essential components of adequate data protection. According to Jasmontaite [9], biometric data must be processed to secure all necessary measures are in place. These measures include a) ensuring that the processing is lawful, fair, and transparent; b) making sure that the purpose for processing the data is specified, explicit, and legitimate; c) imposing restrictions and/or limitations on the processing; d) ensuring the security of the data; e) processing the data accurately and with accountability. As emphasized, appropriate technical measures must be abode to encounter GDPR requirements [7]. To reach transparency, there must be clear messaging about why the data needs to be processed, how it will be processed, and how the automatic algorithms will work.

According to CNIL's responses to questions about biometric regulation from 28 March 2019, this standard regulation also applies to employees, trainees, temporary workers, volunteers, people in civic service, and agents of the three public functions who use biometric data to control access to premises, applications, and professional tools. However, it does not apply to pursuing a purpose other than that of controlling access to the workplace; likewise, according to Délibération n° 2019-001, Article 2, the use of biometric devices is not permitted except for the following purposes within the scope of the Law No. 2018-493: 1) controlling access to specific premises identified by the organization as requiring restricted access and 2) controlling access to professional computing devices and applications identified by the organization.

In this regard, other standard regulations may be documented by the CNIL to govern other processing of biometric data. In practice, it is typical for the design and installation of a biometric access control system to be empowered by a third-party service provider. This service provider will be qualified as a subcontractor because it only acts on behalf of and the instructions of the employing organization: it is the matter of who arranges to install the biometric device and who must be recognized as a data controller. The data controller who wishes to have recourse to a subcontractor must ensure that he only calls on organizations offering sufficient guarantees: a contract reminding them of their respective obligations about data protection that must be inducted between them. Public bodies, including local authorities and ministries, must also comply with the standard regulation if they implement a biometric access control system as an employer. However, the model regulation does not apply to biometric data processing carried out by the state as a public authority, and it also does not apply to the processing of data covered under the police justice and enforcement need. In this regard, businesses shall use unique identity proof only if they genuinely respect human dignity because commercial use of biometrics can lead to the monetization of humans, creating a disproportionate correlation with human biological nature [4].

Consequently, the Délibération n° 2019-001 provides regulations for biometric systems used by employers for access control, equipment, and system login purposes. These regulations cover the purpose of biometric identification, the data collection process, the justification for using a specific identification method, access to biometric data, biometric modeling storage and retention periods, information security measures, and an impact assessment on data protection. The rules require that biometric identification must use a modeler stored in an encrypted form and not the raw biometric data. The reference framework aligns with previous

positions of the CNIL regarding biometrics in the workplace. The new model answers organizations on restraining biometric data processing and is binding.

3. Decision N°AU-007, Decision N°AU-008, and Decision N°AU-019 regardless Biometric Data Processing in a Workplace

The new requirements outlined in Délibération n° 2019-001 are built upon the previous standings taken by CNIL on unique identification in the employment field. Therefore, to better understand the new rulings, it is necessary to consider the prior provisions of the former FDPA, which provide a fundamental framework for regulating biometric data in the workplace. Although these previous Decisions were in effect before the GDPR came into force, the study suggests that the French experience can provide insight into compliance efforts with GDPR Article 9, paragraph 2 (b). In other words, the new requirements of Délibération n° 2019-001 build upon previous regulations and positions taken by the FDPA. Thus, it is important to consider these previous provisions in pursuing to understand the new requirements. Additionally, the study suggests that the French experience in regulating biometric data in the workplace can provide valuable insight for complying with GDPR Article 9 paragraph 2 (b), which outlines the conditions for processing biometric data.

The first Decision, AU-007, on the use of hand geometry to control access to work premises and mass catering or Unique Authorization AU-007 according to Deliberation n°322–2012 of 20 September 2012, pertains to using hand geometry for access control and mass catering in the workplace and is highly relevant to the research topic. This decision authorizes FDPA to regulate all practical forms of biometric data processing, including hand geometry for access control, time and attendance management, and canteen use. The decision also lays down conditions relating to the purpose of processing, technical characteristics, types of data processed, data recipients, retention periods, security measures, and employees' right to access and rectification. These requirements are similar to those set out in the GDPR, specifically in Chapter 3.

The Decision's final requirements do not permit the use of fingerprints for unique identification in the workplace. Instead, hand geometry can be used for access control, time and attendance management, canteen access control, and visitor access control to employees. These purposes can be used separately or combined. Additionally, technical performance requirements for biometric data processing and risk assessments must be followed. The Decision mandates that only the hand configuration, not an image or drawing, can be stored. Moreover, only the geometry of the hand, not its lines, fingerprints, or characteristics, can be used. The Decision specifies that the hand geometry pattern can be stored in a central database, which can be linked to a personal identification number. Additionally, the biometric system can be linked to other applications such as the time and attendance application or the canteen management and payment system. The data collected is divided into five categories: personal data such as name, photograph, ID number, hand geometry template, and professional data such as department and function. The system also records attendance time, movement data, and canteen processing data such as price, payment method, and type of meal. The study notes that this additional data could reveal further personal information about an individual. Companies are only allowed access to data for specified purposes and as part of their assigned tasks. The hand geometry template may only be temporarily disclosed to staff or security personnel for recording or deleting from the database. In some

instances, protected staff members may also access the arrival and departure date of other staff members under applicable regulations. The biometric hand geometry system efficiently manages access control, time and attendance, and canteen usage while adhering to data protection regulations.

Based on the Decision N°AU-008 on the use of fingerprinting exclusively stored in a personal device to control access to professional premises or Unique Authorization, AU-008 under Deliberation n°102–2006 of 27 April 2006, approved biometric systems are those that, based on the matching of fingerprint templates stored exclusively on a data carrier kept by the data subject for access control to certain premises in the workplace. The research hypothesis regards this approach as critical, as in such a case, the fingerprint template would not leave any traces on any registration equipment during the registration process. Besides, the card should be kept under the sole control of the employee. There are also prerequisites laid down in previous Decision N°AU-007 reaching the finality of the processing, the technical characteristics, the type of data, the storage period, security measures, notification measures for workers, and the guarantee of their right to access and rectification. The final requirement is to use a biometric system based on the fingerprint template for access control to specific rooms and areas, including for employees and visitors. The template is a unique biometric key obtained through an algorithm measurement process. Technical specifications dictate that only the fingerprint template can be stored, not the actual fingerprint image. It can be saved on an individual storage medium such as a visionary or magnetic card. The data subject must exclusively control the storage medium, and any incorrect copies must be deleted immediately after the registration phase. Some identifying and badge validity data can be stored on a dedicated access control server, but the fingerprint template is explicitly excluded from such storage. The data linked to the fingerprint are limited to three categories: identification data such as first and last name, photograph, card number, and fingerprint template.

Also, the FDPA has implemented a distinctive solution known as Decision N°AU-019 on the use of vein pattern recognition to control access to professional premises or Unique Authorization, AU-019, Deliberation n°316–2009 of 7 May 2009, which involves the use of vein pattern recognition for controlling access to professional premises. To comply with processing finality requirements, unique identification using finger vein pattern recognition must be made through a system that checks the registered finger vein pattern templates on an individual carrier or reader terminal. This system is solely for access control purposes, specifically for controlling entry to the company and certain restricted rooms within the workplace, as indicated in Article 1. Based on Article 2, the conditions for data processing apply not just to employee data but also to unauthorized visitors. Recent research has demonstrated that the pattern of veins in a person's finger can be captured on a reader terminal or data carrier by the employer. Only those authorized to receive employee data should have temporary access to the template to register it on the card. The new development is that those who receive this information cannot directly access, change, or duplicate an employee's template onto another medium.

The conditions in this regulation are like the previous decisions set out above. That is, there are conditions developed on the finality of the data processing, the technical characteristics and type of data processing, the final recipient of the data, and the retention period. Furthermore, the conditions have been laid down to protect the employees concerning security measures and to ensure that they are informed and have

the right to access and rectify. Also, the template must be stored exclusively in the encrypted form in the memory of the template reading and a comparison terminal that does not have a communication port that allows template extraction. Alternatively, it can be on an individual secure medium, which remains in the employee's possession. The regulation on encryption of the template and the protected object - the carrier is new compared to other solutions.

The new prerequisite is that processing must occur exclusively from the terminal for reading and comparison. Besides, access control should be carried out by comparing the employee's finger and the template available in the system. In the accumulation of fingerprint data, there is a connection to other personal information of the employee that is necessary for identification, as stated in Article 1. Similar requirements have been seen in past decisions, except that N°AU-019 does not include the working card number. This inconsistency could result in errors and incorrect data. N°AU-019 sets forth additional and detailed safety requirements for workers in Article 6, which is a first among all other decisions. For instance, individual access to biometric data is only granted using a password. The password must contain at least eight alphanumeric characters, one number, one letter, and one punctuation mark. The FDPA also mandates the ability to register vein patterns of multiple fingers for each subject. Therefore, according to the research, templates stored on the device must be encrypted for protection since they are difficult to hack, and templates cannot be converted back to the corresponding image.

4. The Unique Identification of Employees under Délibération n° 2019-001 of 10 January 2019

According to GDPR Article 5, data processing must comply with specific criteria, which include lawfulness, fairness, transparency, purpose determination, data minimization, accuracy, storage limitation, and confidentiality. These criteria ensure that data processing regulation is proportionate and address the risks posed to protect individuals' privacy. One of the primary safeguards is purpose single-mindedness, which assures individuals that their biometric data will not be processed unexpectedly. This means only the necessary biometric characteristics should be collected in the required amount. For example, only fingerprint data is needed for fingerprint recognition, and a person can be uniquely recognized from one or two fingerprint characteristics. This principle is essential in protecting individuals' rights to privacy while allowing for the benefits of biometric technology. Therefore, it is necessary to delve into the modern requirements specified in the Délibération n° 2019-001. For this purpose, to protect workers' data, the research strives to clarify what unique characteristics are permitted to be processed under CNIL Délibération n° 2019-001.

Regardless, the research found that biometric characteristics can be divided into three types: morphological, biological, and behavioral. Morphological characteristics include physical features like fingerprints and the shape of the hand, while biological characteristics include bodily fluids and DNA. Behavioral characteristics include things like gait. Given the particularly invasive nature of such procedures, which are only carried out in contexts, for example, paternity actions, and judicial inquiries, the CNIL has decided to exclude their use for specific purposes completely in access control to professional premises and work tools. On the other hand, the Délibération n° 2019-001, Article 5 does not obligate employers to use specific biometric characteristics rather than others, likewise fingerprints, a venous network of one hand, an

image of the iris, and face. Therefore, it is up to the data controllers to make and justify the choice of one or more required biometric characteristics considering the condition when authentication biometrics requires biological sampling, as saliva and blood are prohibited.

The unique characteristics of biometric data and the risks associated with their processing limit the circumstances under which a data controller can effectively use biometric devices in the workplace. When a user is registered in a biometric device, the system measures specific physical, biological, or behavioral characteristics such as fingerprints, iris, or gait. These measurements are stored as a template. The types of templates allowed in the model regulations depend on the control individuals have over their biometric data. In the view of the research, while it may be legitimate for an employer to control access to professional premises, the use of biometric devices must be proportionate and justified by the employer. Employers must show that there is a need to implement a biometric device and that it is the best solution for controlling access compared to other less invasive methods. The company must demonstrate that less intrusive measures, such as badges or access codes, are insufficient or inadequate to employ biometric data processing to pursue an extraordinary title in the workplace. For instance, if there is a need for reliable identification to deter identity theft in case of badge theft or access code interception, then the company must justify the need for more advanced security measures. To achieve the unique identification of workers, the company must provide a specific context that legally requires high protection. For example, this may include addressing dangerous machinery or products, accessing funds or valuables, using equipment or products subject to specific regulations that deal with psychotropic substances or their precursors, or working with chemicals that could be used for weapon manufacturing.

The ruling has categorized biometric devices into three main types to improve readability and clarity. According to Article 4, a biometric access control device can only store certain personal data provided by the employer or employee. This includes: (a) identity information such as name, first name, photograph, raw recordings of biometric features, templates of one or multiple biometric characteristics, authentication numbers or personal support, professional contact information, and encryption keys; (b) professional life details include internal numbers, membership of a body or service, rank, and the identity or corporate name of the employer; (c) access information such as allowed access, zones, and time slots; (d) work tool access, including relevant materials or applications, authorized access terms, and time slots.

The EU concept of human-centric control emphasized to empower individuals to detect and challenge unfair biases and prevent the secondary use of their biometric data. This approach is necessary to protect individuals' fundamental rights while promoting innovation and access to biometric data. In this respect, Délibération n° 2019-001 in Article 7 defines three types of processing according to the control over the operation.

The stipulation outlines the specifications for type (1) biometric devices where the individual solely controls the template. This can be a card or badge with a chip that stores the template. In this type, the storage media for the template is individualized, meaning that a single media can only contain one template and is held by the concerned employee themselves without any copies being retained by the employer or technical service providers. During access control, the employee presents the medium containing the template and the recorded

biometric characteristic, such as an iris or fingerprint, which the device then compares. This device allows for employee identification and authentication, limiting the risk of unauthorized access to their biometric data. Since there is no centralized database of biometric templates for all employees, the risk of hacking is also eliminated.

The type (2) biometric device involves shared control of the template. In this scenario, a database containing the templates of all employees is used, but the data is encrypted to prevent any unauthorized access. Everyone is assigned a personal authentication element to access the data, such as a code or object in their badge, which must be scanned for authentication. Even if the database is compromised due to an external attack or internal data breach, the risk of data exposure for individuals remains low because the data is unreadable without the personal authentication element.

The type (3) biometric device involves the data controller's exclusive control of the template, meaning that all employee templates are stored in a centralized database. Unlike type (1) or (2), the employee has no control over the storage medium and does not have to communicate a secret code or wear a badge for authentication. While this solution has operational advantages, it poses significant employee rights and freedoms risks. In the view of the research, a centralized database increases the potential for data leaks, which could irreversibly expose the biometric data of individuals. Losing a badge or code could severely affect operations, particularly in emergencies. In principle, type 1 storage guarantees the rights and freedoms of individuals and should be the preferred method for storing templates. Other storage methods should only be used in exceptional circumstances substantiated by specific considerations, such as critical environments like nuclear power plants or sterile laboratories. In such cases, companies should be subject to specific regulations to limit the risk of contamination in the production chain. Suppose an employer wants to obtain the consent of their employees to use a biometric device. In that case, they must ensure that employees have genuine freedom of choice and be offered an equivalent alternative solution, such as a badge or password. Employees should be able to choose the option that best aligns with their personal beliefs without any positive or negative consequences influencing their choice.

With respect to the above findings, the study addresses the issue of privacy in the use of biometric techniques and proposes that companies in France should deploy privacy-enhanced technologies. While EU member states and technology developers are responsible for balancing various implications of technological design, the concept of responsibility, in this case, needs to be clarified. To this extent, the study suggests that French legislators deem whether using techniques and data in privacy-enhanced technologies is proportionate to their intended purposes. This raises concerns about the right to personal data protection, and further interpretation is needed to address this issue.

5. Common and Opposite in the French, Dutch, German, and Italian Data Protection Authorities Course regarding Biometrics

Regarding modern techniques like biometrics, the principle of proportionality can be applied by comparing the laws and practices of DPAs in different Member-States. A study has been conducted that examines four countries with well-developed legislation relevant to the topic. The aim is to identify the primary

and contradicted legal aspects and find criteria for proportionality appropriate for unique identification contrasted to discovered above experience in France based on the positions of the DPAs in the selected countries such as Netherlands, Germany, and Italy. The research shows that DPAs need to estimate the risk of interference with fundamental human rights (FHR) concerning biometric data processing. This helps to mitigate risks and ensure uniform implementation of GDPR legislation across different Member-States. Some countries preferred to update their existing legislation, while others adopted new laws. With harmonization, Member-States can adopt biometrically reliable regulations to protect the interests involved, as directed by the Expert Commission on Regulation. The Court of Justice of the European Union (CJEU) in Case C 617/10 Åklagaren v Hans Åkerberg Fransson also stated that the assessment of such regulations must be based solely on the objectives pursued by the competent authorities of the concerned Member-State. The joint position on biometric systems encourages their use as long as the criteria for lawful processing are specified in the law. This is based on the recognition that these techniques can guarantee the protection of individuals' existence and identity, as acknowledged by the CJEU in the Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen case. The DPA supervises compliance with legal rules for data protection within the EU, including personal data processing and handling privacy complaints.

The DPAs are reviewing whether biometric data processing adheres to the principle of proportionality. The study looks at the positions of various DPAs, including the Italian Data Protection Authority (IDPA), the Authorities Persoonsgegevens of the Netherlands/ Dutch Data Protection Authority (AP), and the German Data Protection Supervisory Authority (GDPA). All DPAs agree that the principle of proportionality should be applied to biometric data processing. The IDPA emphasizes the importance of respecting a person's dignity and balancing the need for biometric data processing with the public interest and freedom of personality. The GDPR's data minimization principle should also be considered when processing biometric data, especially when consent is unnecessary for executing a contract. If a contract includes a clause that goes against Italian Civil Code Article 1418, it should be deemed null and void [10].

The FDPA is being implemented effectively by establishing a proportionality balance between the necessity and consent requirements, as explained by Gayrel [8]. This enables the FDPA to approve or reject using biometric systems in the private sector for biometric identification. To ensure compliance with the legislation Délibération n° 2019-00, which sets out a balance of interests criterion, further restrictions have been imposed, particularly about the processing, usage, and storage of biometric data. This legislation serves as a simplified declaration and a practical example of the implications of GDPR at the national level. Given the sensitivity of biometric data, the FDPA has imposed strict obligations on data controllers regarding the configuration of biometric data processing in proportion to the purpose of the processing. These obligations are expressed as follows: Firstly, the processing of biometric data must be strictly limited to access control of premises that require restricted access or access control to a limited number of devices and IT professional applications, which the organization must identify. Secondly, the organization must demonstrate that it is impossible to achieve the above purposes by means other than processing biometric data. Thirdly, the data controller must document why such a high level of protection is needed given the context at hand and why the processing of biometric data is the most appropriate means to ensure security for the company.

The direction of the AP is to ensure proportionality in the sharing of biometric technology between private and public interests. For instance, the Opinion Gezichtsherkenning (2004) permits the processing of biometric data through face recognition for security purposes, such as gaining access to public meetings. This is because the Netherlands recognizes the use of biometric systems for unique identification purposes in cooperation with the **Netherlands** Organisation for Applied Scientific Research **- Physics and Electronics** Laboratory. This specification was made before the implementation of GDPR to comply with Directive 95/46/EC. At the national level, if the previous legislation adopted under Directive 95/46/EC does not contradict the norms of biometric data processing based on GDPR and instead strengthens the protection of individual rights within the scope of unique identification, then such norms remain in force. According to the analysis, biometric technologies are mainly oriented toward private interests, as they could be more usable in public contexts. This position supports the idea that businesses are exploring biometric technologies more than the state for their benefit.

To minimize the risks associated with using biometric technologies in a private context and to confirm the protection of biometric data processing, the AP suggests using Privacy Enhancing Technologies (PET). Under the research, PET can help minimize the risks of violating Article 7 of the CFREU and provide better protection while meeting the requirements of GDPR, even if supervision fails. This is because PET aids in balancing private entities' interests with individuals' rights in biometric data processing. The GDPA supports the use of PET but strictly prohibits the benefit of biometric data processing by PET, especially for commercial purposes, as noted by Paul de Hert [14]. The main reason for this is that the aim of BDP can often be achieved through other means, as stated by Štitilis [16]. Therefore, there is no legal justification for using biometric technologies in private areas, according to Štitilis [16]. For example, even images of fingerprints stored on a passport's microchip must be deleted from the database immediately after the document is issued. Identity forgery is risky if such information is kept in the system.

The study has shown that contradictions arise due to differing interpretations of application direction, regardless of the processing needs that must be supervised. It pleads that parties must assess whether it is necessary to process personal biometric data before applying proportionality. This assessment is a prerequisite for proportionality assessment. However, in practice, it is challenging to demonstrate that processing BD is strictly necessary for the intended purpose. Controllers may only be vested with this task in exceptional circumstances, such as accessing a football stadium. Without special safeguards, demonstrating necessity becomes a subjective matter of interpretation. Additionally, it may require unique identification of individuals in specific circumstances, times, and places. It is crucial to determine whether and under what conditions this objective justifies reducing the fundamental right to data protection and whether it is proportionate to interfere with privacy. The decision cannot be taken by the DPA alone and must also be subject to additional legislation on a national level.

Regarding the legal method of applying proportionality, the FDPA displays that the AP's position on allowing unique identification for security needs is deemed non-proportional. This is because the distinction between security needs should not only be based on the private entities' interests but also on pressing security goals and identity management purposes. Therefore, the AP guidelines recommend that private entities limit

the number of authorized personnel. It is important to note that, in the case of security techniques, dimensions must be abode to prevent linking information about the source of biometric characteristics, as the primary source is a human, and other types of personal data may be disclosed during biometric data processing.

A strict stance exists regarding the implementation of biometric technology that is inherently governmental and may be compelled to safeguard national interests such as national security, counterterrorism, and visa issuance. However, the FDPA contradicts this stance by emphasizing that security measures must be exceptional and necessary, exceeding the interests of the controller and protecting the physical integrity of individuals. This pertains specifically to security needs that require higher measures of protection. The research concludes that controllers may rely on higher security interests to protect the interests of others. The FDPA allows controllers to process biometric data to secure access to places rather than positions of authority.

Another specific contradiction concerns the ongoing discussion on balancing interests. The AP frames that collecting data on third-country nationals is a legitimate aim of a controller to maintain order and safety, per the final Commission, Implementing Decision on technical specifications regarding the standards for security features and biometrics of 30 November 2018. However, according to the manuscript, the reference to personal safety does not equate to public safety under the CFREU, Article 52. From the perspective of the DPA, a person should be informed, and the private party must provide information about the processing. In this regard, the person's biometric data must be controlled for each applicable purpose. Decentralized unique identification remains the person's possession to the loss of anonymity, as noted by Kindt [11]. Knowledgable, in Germany, there is a practice where the GDPA in 2004, within the German Olympic team participation in Athens, admitted security matters through biometric extracts. Certified guests of the Olympic crew were given unique ID tags that included the person's fingerprints. Hence, both AP and GDPA mention alternative identification methods, but they are overall limited. Consequently, the research claims that the earlier idea about adopting legislation in relation to technical concepts of the PET is relevant.

The position of DPAs regarding the criterion of purpose limitation for biometric operations is also problematic, as they need to apply it uniformly. The FDPA and AP have contradictory positions on a similar detail, such as the procedure of fingerprint processing. To avoid conflict with CFREU Article 7, the AP uses an alternative method called a smart object holder, which carries finger characteristics. This means the person can put their finger on the machine without putting their finger on the machine. The FDPA's explanations are a condition before the safeguards for using human characteristics that do not leave traces, which could balance interests. This safeguard can be used to mitigate risks because the practice commonly uses the characteristics of a finger, which, due to its nature, leaves an imprint. Using an intelligent object holder is recommended to address the issue of characteristics that leave traces. This solution also aligns with the GDPA's application to confidentiality and integrity in biometric systems. However, the FDPA has a different opinion on this solution, as seen in its Opinion N° 04-018 on the request for an opinion by the Hospital of Hyères relating to the employment of a fingerprint verification application for the management of employee's time and attendance in 2004. The FDPA is concerned that the database will store samples for later use, which could compromise data protection.

To define, it is essential to distinguish between biometric data that leaves a trace and biometric data that does not leave a trace. Legal safeguards must be properly balanced, prioritizing biometric data that does not leave a trace. The FDPA proposes employing hand geometry and vein characteristics, which do not leave a trace. Proportionality must also be devoted to storage, with consideration given to the place of storage for such unique characteristics. To restate, there are two feasible solutions for balancing the storage of biometric data: a central storage server of the private entity or the reader/other objects under an individual's control. The FDPA proposes using hand geometry and vein as unique characteristics that do not leave traces and suggests applying proportionality to storage matters. Personal access via code stored together with the template is recommended. The IDPS clarifies that balance must be complied with via e-indexing the information. The AP imposes a limitation on BDP through a storage requirement that biometric characteristics must be reserved within 24 hours in a central database and removed. The FDPA refers to the general rule that biometric data shall not be kept longer than necessary. The approach of the Netherlands is considered beneficial in achieving the implementation of additional measures.

6. Conclusions and Recommendations

The research position concerns the criterion of a legitimate basis for processing biometric data in a workplace. The study associates the legitimate basis proportionally to the position of the person. It distinguishes and rules a legitimate basis for two categories: employees and security have a legitimate basis, while enrolled e-users of biometric e-tools have a legitimate permissible basis. For the latter category, individual consent is strictly necessary. The legitimacy of the basis is an explicit and purposeful ground provided only by a legislator. As such, national law shall forbid processing in an incompatible way, such that the unique identification process does not reveal data relating to health, race, etc. The research position could be emphasized by legitimizing the criteria used regarding the biometric system.

Based on the findings, the manuscript proposes a distinction for processing biometric data of employees based on two criteria. The first is security, where the person cannot opt out of such processing, and consent is not required to be taken by the company. The second is identification for convenience purposes, where the person's consent must be brought, and a private entity cannot claim security as the basis for processing. In case of a person's refusal, an alternative for further access should be made available to them.

Assuming that Data Protection Authorities are concerned about the criteria of proportionality, it is strongly recommended that biometric data processing be evaluated under the proportionality test proposed by the European Data Protection Supervisor's Guidelines on Assessing the Proportionality Measures that Limit the Fundamental Rights to Privacy and the Protection of Personal Data of 19 December 2019. This proportionality test is a set of guidelines that assists in setting the mark of criteria that cap fundamental rights to privacy and personal data protection. It comprises an exhaustive analysis of the measure's legality, legitimacy, and proportionality, weighing the specific context and circumstances of processing private data. By operating this proportionality test, DPAs can confirm that unique identification is used appropriately and proportionally to counteract the data subjects' interests with the data controllers' legitimate interests.

Transparency in biometric data processing refers to the obligation of organizations to provide clear, understandable, and easily accessible information to individuals and data protection authorities. This includes details on why and how biometric data needs to be processed and the use of automatic algorithms and predictions related to the nature of the biometric data. On the other hand, accountability involves conducting independent audits on biometric data processing and taking necessary bars when needed. This cannot be replaced by self-regulation and must be complemented by designing goods, services, and applications prioritizing biometric protection through design and default. This responsibility should be integrated into the current GDPR framework, and hardware or software solutions should be chosen carefully while respecting individuals' dignity.

Therefore, the manuscripts offer recommendations for countries open to updating data protection law in the context of permission unique identification, which should include several key provisions. Firstly, it should require organizations to justify their use of biometrics based on specific considerations such as context, risks, and technical and regulatory constraints, especially for biometric types that pose the most significant risks. Secondly, the regulation should impose rigorous requirements for organizational and technical security measures to protect personal data. Thirdly, organizations should be required to document their decision-making process and justifications when deploying biometric devices. Fourthly, the regulation should reinforce GDPR obligations, including the requirement to inform individuals about the use of their data.

The manuscript presents a valuable table [3], 'Risks Mitigation of Biometric Data Processing based on the Principle of Proportionality Application,' to assess the risks of biometric data processing by applying the principle of proportionality. Among exemplified risks are: 1) uncertainty on the necessity; 2) conflicting interests; 3) respect for privacy; 4) data disclosure and processing for incompatible purposes. Accordingly, the table consists of several steps that need to be considered, including but not limited to the mitigation methods based on 1) the legitimacy or legal ground for the unique identification under GDPR Article 9, 2) the balance of interests involved via a common consent, 3) purpose limitation with stress to the storage and database used, 4) assessment technical and organizational measures via the condition of unique type characteristics taken.

Table. Risks Mitigation of Biometric Data Processing based on the Principle of Proportionality Application

STEPS	**Disadvantage**	**Mitigation** ⇨	**Purpose**	**Resulti** ⇦
	Risks	**Principle of the Proportionality**	**Biometric Data Processing**	**Compliance**

1	Uncertainty on the Necessity	Legitimacy	Identification / Authentication / Verification	Unique identification. GDPR Article 9 (1). It is an Identification or Authentication procedure. It is applicable if more than Verification is needed to identify as a non - unique recognition method.
2	Incompatible Interests	Balance of Interests	Consent	Free of choice with respect to Human Dignity under the Charter Fundamental Rights of the European Union Article 1.
3	Privacy to Charter of Fundamental Rights of the European Union Article 7 Respected	Purpose Limitation	Storage	Decentralized.
			Biometric Database	At any time, a person shall realize the right to check a biometric data statement in the system. GDPR Article 21. It is possible under the EU's regulative concept of Personal Information Management System (PIMS) designed for online identity management.
4	Disclosing other categories of Data, and Processing for Incompatible Purposes	Technical and Organizational Measures	Biometric Data leave traces VERSUS do not leave traces	Specific safeguards for biometric data that leave traces, like fingerprints. For example, the print can be in a material sensor holder. That is, a person applies not a finger itself to the biometric system but a material object with the biometric characteristics of a finger.

Under the table [3], 'Risks Mitigation of Biometric Data Processing based on the Principle of Proportionality Application,' the biometric identification concedes with the GDPR framework following the next statements: 1) to determine when GDPR Article 9(1) does not apply, it is essential to implement an identification or authentication procedure that enables the unique identification of an individual. This becomes necessary when non-unique recognition methods are insufficient and a more robust verification process is required; 2) according to the Charter of Fundamental Rights of the European Union, Article 1 guarantees freedom of choice for individuals while respecting their human dignity. This means that individuals have the right to make choices and decisions, without any coercion or undue influence from others, in a manner that upholds their inherent worth and value as human beings. The study emphasizes the need for ensuring informed consent, alternatives for refusal, and maintaining transparency in the processing of biometric data; 3) Decentralized storage is a method of storing data that can improve privacy by distributing information across multiple locations rather than storing it in a single central location. Additionally, under GDPR Article 21, individuals can access and review their biometric data anytime. Additionally, the manuscript recommends that this can be facilitated by implementing a Personal Information Management System (PIMS) under EU regulatory concepts. By using a PIMS, individuals can better manage their online identities, including their biometric data, while protecting their privacy rights; 4) Specific safeguards must be implemented to protect individuals' privacy when dealing with biometric data, such as fingerprints. One approach is to use a material sensor holder, which allows a person to apply a material object with the biometric characteristics of a finger to the biometric system instead of the finger itself. This method can help to prevent the collection and storage of actual fingerprints, which can leave traces that could be used to identify individuals. By using a material sensor holder, individuals can have their biometric data captured and stored in a way that is less likely to be used for malicious purposes. This is just one example of how specific safeguards can be put in place to protect biometric data and the privacy of individuals.

The comprehensive contribution is that - by following the steps presented in the table ‘Risks Mitigation of Biometric Data Processing based on the Principle of Proportionality Application’ and adhering to the principle of proportionality, organizations, companies, institutions, authorities, and other persons that desire to employ biometric technology - can confirm that their biometric data processing practices are lawful, ethical, and respectful of individuals' privacy and data protection rights.

References

1. Brkan, M. (2016). The Unstoppable Expansion of EU Fundamental Right to Data Protection. Little Shop of Horrors? Maastricht Journal of European and Comparative Law, 23(5), 812–841. URL:https://doi.org/10.1177/1023263X1602300505
2. Brumnik, R. and Podbregar, I. (2010). Biometric Technology and Human Rights. US-China Law review, 7 (1).

3. 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 Dissertation, 1-371.
4. Bulgakova, D. (2022). Case Study on the Fingerprint Processing in a Workplace under GDPR Article 9 (2, b). Teisė, 124, 22-38. URL:https://doi.org/10.15388/Teise.2022.124.2
5. Bulgakova, D. (2022). The Protection of Commodified Data in E-Platforms. *Analytical and Comparative Jurisprudence*, 1(2022), 208–212. URL: https://doi.org/10.24144/2788-6018.2022.01.39
6. Blazy, O., & Yeun, C. Y. (2019). Blockchain and the GDPR: A Data Protection Authority Point of View. In Information Security Theory and Practice (Vol. 11469, pp. 3–6). Springer International Publishing AG. URL:https://doi.org/10.1007/978-3-030-20074-9_1
7. Duque de Carvalho, S. L. (2019). Key GDPR Elements in Adequacy Findings of Countries That Have Ratified Convention 108. European Data Protection Law Review (Internet), 5(1), 54–64. URL: https://doi.org/10.21552/edpl/2019/1/9
8. Gayrel, C. (2016). The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations. The Computer Law and Security Report, 32(3), 450–461. URL: https://doi.org/10.1016/j.clsr.2016.01.013
9. Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., & Leucci, S. (2018). Data Protection by Design and by Default. European Data Protection Law Review (Internet), 4(2), 168–189. URL: https://doi.org/10.21552/edpl/2018/2/7
10. Kindt, E. (2007). Biometric applications and the data protection legislation: The legal review and the proportionality test. Datenschutz Und Datensicherheit, 31(3), 166–170. URL: https://doi.org/10.1007/s11623-007-0064-6
11. Kindt, E. (2012). The Processing of Biometric Data, A comparative Legal Analysis with a focus on the Proportionality Principle and Recommendations for a Legal Framework. Doctoral thesis.
12. Lubin, A. (2020). The liberty to spy. Harvard International Law Journal, 61(1), 185–243.
13. Milaj, J. (2016). Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance. International Review of Law, Computers & Technology, 30(3), 115–130. URL.https://doi.org/10.1080/13600869.2015.1076993
14. Paul de Hert & Christianen K. (2013). Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data. Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.
15. Sprokkereef, A. (2007). Data Protection and the use of Biometric Data in the EU. The Future of Identity in the Information Society, 277–284. URL:https://doi.org/10.1007/978-0-387-79026-8_19
16. Štitilis, D., & Laurinaitis, M. (2017). Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law. The Computer Law and Security Report, 33(5), 618–628. URL:https://doi.org/10.1016/j.clsr.2017.03.012

17. Taylor, M. (2015). "Safeguarding the Right to Data Protection in the EU," 30th and 31st October 2014, Paris, France. Utrecht Journal of International and European Law, 31(80), 145–152. URL: https://doi.org/10.5334/ujiel.cw
18. Worku, U. (2016). The Feasibility of Applying EU Data Protection Law to Biological Materials: Challenging Data as Exclusively Informational. Journal of Intellectual property, Information Technology, and Electronic Commerce Law, 7, 97.