交大法學評論，第 14 期，頁 61（2024）

Facial Recognition at the Fitness Center Under the General Data Protection Regulation Article 9(1) and 9(2)(a)

Daria Bulgakova [*], Valentyna Bulgakova [**]

Abstract

There are significant concerns regarding the legitimacy of biometric data processing within the European Union. Therefore, it is imperative that facial data processing adheres to the criteria and standards outlined in the General Data Protection Regulation (GDPR).

According to GDPR Article 9(1), the processing of biometric data is prohibited. In high-incursion situations that involve the private sphere, obtaining consent becomes crucial. It requires further justification and confirmation about the

[*] Ph.D. in International Law, Advocate of Ukraine, Dnipropetrovs'k Regional Bar Council, Kryvyi Rih, Ukraine. Email: dariabulgakova@yahoo.com; ORCID: https://orcid.org/0000-0002-8640-3622.
Дар'я Анатоліївна Булгакова, Доктор Філософії з Міжнародного Права, Адвокат, Кривий Ріг, Україна.

[**] Pedagogue-Methodist of the Highest Category, Kryvyi Rih, Ukraine. Email: krotona24@gmail.com; ORCID: https://orcid.org/0009-0009-6463-5228.
Валентина Анатоліївна Булгакова, Педагог-Методист Вищої Категорії, Кривий Ріг, Україна.

lawfulness of the process, as specified in GDPR Article 6. Hence, the European Union relies on Data Protection Authorities in Member States to assure obedience to GDPR in practice.

Regardless above mentioned, the authors aim to investigate compliance with the GDPR Article 9(1) and 9(2)(a) through the case study about facial recognition technology with biometric involvement at a fitness center in Denmark.

The research focuses on analyzing the Danish Data Protection Agency's investigation of FysioDanmark concerning the facial biometric recognition of customers' and employees' faces at the entrance to a fitness center for membership control checks and business optimization. The authors have made the following findings. The Agency warned the entity in question about the use of a system in fitness centers to uniquely identify customers without obtaining their consent. Furthermore, the research has shown that the application of consent as a legal ground to avoid prohibition to uniquely identify employees can't be granted as an appropriate argument due to an imbalance of employment relationships meaning the consent is not freely given.

Based on the given outcomes, the authors propose measures to prevent

Acknowledgments. The authors are thankful for the useful advice about the practical understanding of the GDPR Articles 51, 57, and 58 given by Tetiana Leshchenko, Head of the Dnipropetrovs'k Regional Bar Council, Dnipro, Ukraine. The opinion of Tetiana Leshchenko became significant to comprehend the role of the Danish Data Protection Authority (DPA) concerning fitness center FysioDanmark.

Подяка. Автори роботи "Практика Розпізнавання Облич у Фітнес-Центрі відповідно до статті 9(1) та 9(2)(a) Загального Регулювання Захисту Даних" вдячні за корисні поради щодо практичного осмислення статей 51, 57 та 58 Загального Регулювання Захисту Даних (GDPR), надані Тетяною Олександрівною Лещенко, Головою Ради Адвокатів Дніпропетровської області, Дніпро, Україна. Думка Тетяни Олександрівни є значимою у розумінні діяльності Датського органу із нагляду у дотриманні захисту даних (DPA) у фітнес-центрі FysioDanmark.

投稿日：2023 年 3 月 30 日；採用日：2023 年 5 月 21 日

noncompliance with biometric facial technology and advocate respect for individuals' right to personal data protection by mandating consent for facial recognition, specifically for the purpose of unique identification, prior to the performance of facial biometric scans. And, the authors' advice is not to regard the GDPR Article 9(2)(a) in terms of biometric facial employees' data processing because it is not a legal ground to exempt from Article 9(1) at the fitness workplace center.

Keywords: GDPR, Unique Identification, Biometrics, Control Entry Management, Consent, Public Interest.

1. INTRODUCTION TO THE REGULATORY APPROACH

The challenge with biometric data, despite its clear prohibition to process under GDPR[1] Article 9(1), is that individuals, as outlined in Article 5(1), must be fully informed about the specific technological features directed to work with personal data clearly and transparently. Additionally, as noted in Recital 42, any written declaration of consent must ensure that individuals know the extent to which they give consent and any related safeguards. Individuals should understand the controller's identity and the biometric processing's intended purposes before as to consent which cannot be considered freely given if an individual feels coerced, lacks a genuine choice, or faces the not balanced and forced consequences in the event of refusal or withdrawal data authorization agreement.

The need for translucence is particularly crucial in cases where facial identification systems are utilized for control entry matches. In high-stress scenarios, such as security entrance measures, the legitimacy of the unique identification act becomes opaque. Interoperability further complicates matters as transparency regarding the purpose of facial identification encourages individuals to engage with the authorization process and prevent situations from escalating. The obligation to notify shall be embedded in the policy of all information technology approaches. The European Union (EU) counts on the work of Data Protection Supervisory Authorities settled in the Member States to harmonize the data protection force and confirm compliant work as per the GDPR Article 51.

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119).

Besides, according to Article 51 para 2, the member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers, remain free from external influence, whether direct or indirect and shall neither seek nor take instructions from anybody to exercise tasks having investigation power as per Articles 57 and 58.

According to the GDPR Article 21, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defense of legal claims.[2]

Yet, in the view of the research, the GDPR rules are not enough to understand the implementation of Article 9(1) concerning biometric data especially when facial recognition technology (FRT) is demanded across the globe. Since the EU law is lack specific guidelines about facial recognition, it is visible to look at the international conceptualization of FRT which could if not clarify the legitimacy of facial identification practice by the private sector in the EU but instruct the key aspects that research demands to investigate of the unique facial recognition actual state. Thus, according to the Regulating facial recognition in the EU,[3] which

---

2 Furthermore, under the GDPR Article 79 para 1, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with GDPR.

3 TAMBIAMA MADIEGA & HENDRIK MILDEBRATH, EUR. PARL. RSCH. SERV., REGULATING FACIAL RECOGNITION IN THE EU (2021), https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf.

explores the current EU legal framework applicable to facial recognition and examines the recent proposals for regulating facial recognition technologies at the EU level in-depth, in 2020, the United Nations (UN) Human Rights Council adopted a resolution specifically condemning the use of FRT in the context of peaceful protests, since these technologies create a chilling effect on the exercise of the right to protest by enhancing governments' abilities to identify, monitor, harass, intimidate, and prosecute protesters.[4] The Council called on states to refrain from using facial recognition technology to monitor individuals involved in peaceful protests. Furthermore, the Council of Europe (COE), the Strasbourg-based European human rights organization adopted the Guidelines on facial recognition.[5] Nevertheless, the guidelines are general in scope and cover the uses of facial recognition technologies in both the private and public sectors, yet, the COE Guidelines, in the authors' view, could be taken for the model since it stresses the use of FRT, including live facial recognition technologies; provide a set of reference measures that governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies should follow and apply to ensure that they do not adversely affect the human dignity, human rights and fundamental freedoms of any person, including the right to protection of personal data. The guidelines do not exclude that further protective measures may be required in the applicable legal framework depending on the particular use of the technology.

There are several relevant reports for the research attention of the European

4 Human Rights Council Res. 44/20, U.N. Doc. A/HRC/44/L.11 (July 13, 2020).

5 CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (CONV. 108), COUNCIL OF EUR., GUIDELINES ON FACIAL RECOGNITION 29 (2021), https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.pdf.

Union Agency for Fundamental Rights (FRA)[6], and the Consultative Committee of the Convention 108.[7]

At the last, it is important to understand the techniques and methods of FRT to prove that toils with biometric data. Besides, authors' eyesight is that society encounters intensive processing of biometric data, which thus poses situations of high incursion into the private sphere. The presented case study of FysioDanmark displays the course of not a simple authentication but rather a unique identification at the gate of the entity that requires double legitimation. Reasonably, the research offers below significant understanding of three FRT varieties to find out the appropriate biometric means in terms of the GDPR Article 9(1) and 9(2)(a) further.

Thus, *facial identification* or designation is a technique of reaching an individual's facial shot with templates of different people reserved in a database to confine the identicalness of the individual in that shot. This method is exploited to pinpoint individuals in varied contexts, largely for security and law enforcement conditions. Facial algorithms could tag diverse segments of the face. At the same time, an algorithm is a method, an ordered set of operations, or a recipe and not a means to store biometric data. It means facial identification could be done without the process of working with a biometric data of a person concerned as long as this function does not go beyond identification that led to unique (biometric) data workflow with further labeling of a person's distinctive traits. *Facial authentication* is a function of substantiating that a person is who he contends to be

6 EUR. UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), UNDER WATCHFUL EYES: BIOMETRICS, EU IT SYSTEMS AND FUNDAMENTAL RIGHTS 5 (2018), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf.

7 SANDRA AZRIA & FRÉDÉRIC WICKERT, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (CONV. 108), COUNCIL OF EUR., FACIAL RECOGNITION: CURRENT SITUATION AND CHALLENGES (2019), https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1.

by approximating his facial template of the shot with an already comprehended template kept in a database to inspect if his face matches a pre-existing record. This function is usually employed in household technology for security and access control systems, for example, unlocking a smartphone via facial credit or accessing a home facility via facial validation. *Facial verification* is a function of analogizing two templates of the same person to decide if they are a match. It is used to affirm the already known identity for a broad system by capturing a "live image". For example, it is practiced logging into bank accounts or inscribing into social media profiles. Lastly, in the long term, technological interoperability may have the practical effect that certain types of biometric data will be used as a standard single identifier.[8] An aggravating factor could be that unlike personal identification numbers, which can be changed during one's lifetime, such changes are clearly not feasible when it comes to people's biometric data and still less to their faces.[9]

1.1 Case Background

1.1.1 FysioDanmark Case of 2022[10]

The FysioDanmark Hillerød ApS's (FysioDanmark), a Danish company, planned to implement a facial recognition system for seamless entry to its gym for customers and employees eliminating the need for cards or passwords. The system would employ a camera at the fitness center entrance, capable of scanning faces and comparing them with pre-stored photographs in the database. It was intended to be an opt-in system, whereby customers or employees would need to provide their consent to be registered in the system and have their faces captured. Apart from facilitating access to the fitness center provided for customers with

8 *Id*. at 14.

9 *Id*.

10 Danish Data Protection Agency v. FysioDanmark Hillerød ApS's, No.2021-431-0145 (Den. Mar. 17, 2022).

memberships and respective staff members, the facial recognition system was also designed to gather customer data for statistical and business optimization interests. Accordingly, on 7 July 2021, the Danish Data Protection Agency (DDPA) started an investigation on its own initiative concerning FysioDanmark regardless of the intended use of a facial recognition system to uniquely distinguish individuals at the entrance.

Furthermore, the research shows the collaboration between FysioDanmark and Justface ApS on 24 September 2020 in terms of facial recognition service where the first party is responsible for personal data processing, while Justface ApS is the data processor. And, in terms of the FRT functionalities, the system has yet to be activated. It operates by placing a camera at the gym entrance, which captures the faces of customers and employees and further compares them with the previously stored facial biometric data in the system on the way to uniquely determine an individual while penetrating and doorway the fitness center. Once activated, the FRT is in endless online mode without interruption. Those customers who are wishing to use the system for the entry check mechanism must first have their picture taken and uploaded, either physically at the center or online. The FysioDanmark also explains organizational measures taken in asking for electronic consent respectively as well as about the entirely voluntary participation in the FRT solution.

After examining the case details and the information provided by the company, the DDPA concluded that if the system would rely on the customers' (data subjects) consent, then it could be utilized in compliance with the GDPR Article 9(2)(a), and cautioned about the practice of the facial recognition system to uniquely identify an individual without obtaining client consent would presumably contravene the GDPR. Moreover, the DDPA warned that it would violate GDPR rules if the company failed to make sure that the FRT was not used individuals' unique data without consent.

Therefore, the FRT is noncompliant with the GDPR when biometric data is processed to uniquely identify a client without obtaining consent from that data subject in pars of the GDPR Article 9(2)(a), and when such purpose is accomplished for statistics and business optimization. Hereinafter, the force of the GDPR Article 9(2)(a) is legitimately expected in the FysioDanmark "eyes" in the scenario of FRT (to uniquely identify) to improve statistical analysis and meet business efficiency. It is also meaning, the FRT intended processing of biometric data to uniquely distinguish a natural person who did not wish to authorize another party (business) to the process of facial data, is prohibited by Article 9 para 1 as no exception to this scenario can be applicable under para 2.

1.1.1.1 A Consent of FysioDanmark

The authors consider it necessary to assess the FRT consent at the FysioDanmark because it is significant for the practical implementation of the GDPR Article 9(2)(a) as well as the party in question argues that obtained from customers' consent meets the criterion of validity because the designed form includes:

- ✓ highlighted voluntary condition;
- ✓ proposed the option of revocability at any time;
- ✓ information on the FRT purposes with boxes to consent to each purpose separately;
- ✓ a reference to additional information on how FysioDanmark processes personal data.

The research proposes to check the mentioned elements out by looking at the content of the consent in question[11] as follows:

"*Declaration of consent.* I *consent* to FysioDanmark Hillerød, Milnersvej 39,

11 *Note* The highlights and translation of the displayed consent done by authors for the research and, therefore, the exemplified text and design of the consent could differentiate from the original design and language means.

3400 Hillerød *by ticking the consent boxes* below to process the following personal data about me for the purposes described below. FysioDanmark Hillerød encourages me to read the consent declaration form carefully before approval.

I hereby consent to FysioDanmark Hillerød process my personal data about the following:

What *categories of personal data* are processed? General personal data (we only request this information if it is not already filled in at your fitness center): name, birthdate, address, email, portrait image of confidential and sensitive personal data as biometric data in the form of a facial scan.

For what purposes is your personal data processed? Your personal data is processed to verify the validity of your membership when accessing the fitness center.

How is your personal data collected? We collect your personal data from your fitness center user profile in the way that we are asking you to update information about yourself via your profile created in our app or website. This is to ensure that the fitness center always has the correct data on its members.

A biometric scan is performed at the entrance of the fitness center. The scan is for comparison of your picture with the profile picture you have uploaded to your user profile at the fitness center so that we can validate your membership at the fitness center.

How is your personal data processed? Personal data processing is based on Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data (GDPR) and the Danish Data Protection Act. Your personal data will be disclosed to the fitness center you attend and the fitness center's (data) management company – it can be FlexyBox ApS, Sport Solution A/S, or Globus Data ApS. Those in each

case are responsible for processing your data in the base of their own system. We, therefore, also refer to the fitness center's and management companies' respective personal data policies for further information about their personal data processing. Justface will process your personal data in accordance with the purposes described above and only to the extent strictly necessary. Your personal data will only be accessible to relevant and specially designated persons at Justface and will only be disclosed to others if required by the purposes described or if required by law. Further information on Justface's privacy policy can be found on our website: www.justface.dk [...]

Withdrawal of consent. It is voluntary to give consent, and you are entitled to revoke your consent at any time. If you wish to withdraw your consent, simply contact Support@justface.dk, who will then contact the fitness center and the management company to register that your consent has been revoked.

If you do not wish to give consent, or if you withdraw your consent, it is impossible to use biometric scanning, and we hereinafter ask you to contact your fitness center to hear about alternative solutions.[...][12]"

12 **The presented consent is available on the original designed language as follows: "Samtykkeerklæring Jeg giver ved afkrydsning af samtykkeboksene nedenfor mit samtykke til, at FysioDanmark Hillerød, Milnersvej 39, 3400 Hillerød behandler følgende personoplysninger om mig til de nedenfor beskrevne formål. FysioDanmark Hillerød opfordrer til, at samtykkeerklæringen læses grundigt igennem, inden der afgives samtykke. Jeg giver hermed samtykke til, at FysioDanmark Hillerød må behandle mine personoplysninger til følgende formål:**

Hvilke kategorier af personoplysninger bliver behandlet? *Almindelige personoplysninger (vi anmoder kun om disse oplysninger, hvis de ikke allerede er udfyldt hos dit fitnesscenter)*: Navn, Fødselsdato, Adresse, E-mail, Portræt billed *Fortrolige og følsomme personoplysninger* Biometriske oplysninger i form af ansigtsscan Til hvilke formål behandles dine personoplysninger? Dine personoplysninger behandles til det formål at føre kontrol med gyldigheden af dit medlemskab ved adgang til fitnesscentret. Hvordan indsamles dine personoplysninger? Vi indsamler dine personoplysninger fra din

Additionally, the FysioDanmark gave the next altercation. Customers who do not choose the FRT can instead use a physical access card and password, signifying their facial recognition data will not be processed. In such cases, the FRT utilization could be explained similarly approximated with ordinary video surveillance, except that the surveillance images are not stored in the system's memory and cannot be accessed or monitored by the fitness center or Justface.

---

brugerprofil hos fitnesscentret og fra dig selv på den måde, at du vil blive bedt om at opdaterer dine oplysninger via din brugerprofil i vores app eller hjemmeside. Dette er for at sikre, at fitnesscentret altid har de korrekte oplysninger på deres medlemmer. Biometrisk scan sker ved indgangen til fitnesscentret. Scanningen benyttes til at sammenligne dit billede med det profilbillede, du har uploadet til din brugerprofil hos fitnesscentret, så vi kan validerer dit medlemskab hos fitnesscentret. Hvordan behandles dine personoplysninger? Behandling af personoplysninger sker med hjemmel i Europa-Parlamentets og rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (GDPR) og den danske databeskyttelseslov. Dine personoplysninger vil blive videregivet til det fitnesscenter, du benytter, samt til fitnesscentrets (data)administrationsselskab – det kan være FlexyBox ApS, Sport Solution A/S eller Globus Data ApS. Disse er i hver enkelt tilfælde ansvarlige for behandlingen af dine data i deres egne systemer. Vi henviser derfor også til fitnesscentrets og administrationsselskabernes respektive persondatapolitikker for nærmere information om deres behandling af personoplysninger. Dine personoplysninger behandles af Justface i henhold til formålene beskrevet ovenfor, og kun i det omfang, det er strengt nødvendigt. Dine personoplysninger vil kun være tilgængelige for relevante, og særligt udpegede personer hos Justface, og vil kun blive videregivet til andre, hvis det er påkrævet i henhold til de beskrevne formål eller hvis det kræves ifølge lovgivningen. Yderligere oplysninger om Justface privatlivspolitik kan ses på vores hjemmeside: www.justface.dk […] Tilbagekaldelse af samtykket Det er frivilligt at afgive samtykke og du er til enhver tid berettiget til at tilbagekalde dit samtykke. Hvis du ønsker at tilbagekalde dit samtykke, skal du blot rette henvendelse til Support@justface.dk som herefter vil kontakte fitnesscentret og administrationsselskabet for at registrere, at dit samtykke er tilbagekaldt. Hvis du ikke ønsker at give samtykke, eller hvis du tilbagekalder dit samtykke, så er det ikke muligt at benytte biometrisk scan og vi beder dig derfor kontakte dit fitnesscenter for hører om alternative løsninger. […]"

2. RESEARCH DISCUSSION

2.1 The Consent Ground in the FysioDanmark Case

2.1.1 Access Control Solution at the Fitness Center for Customers

The use of FRT for access management is becoming more prevalent, and it is essential to ensure that it is used lawfully. As per the GDPR rule of Article 2(1), the regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Thus, the authors pay special attention to the event when FRT does not manufacture to work with biometric data. Hence, the application of Article 6(1) is especially necessary since the stipulation precisely stipulates the list of conditions when processing is lawful where only if and to the extent that at least one applies. For instance, point (a) clarifies that the processing shall be lawful when the data subject has given consent to the processing of his or her personal data for one or more specific purposes. However, a prohibition on the processing of special categories of data, including biometric data,[13] for the purpose of uniquely identifying a natural person, is stipulated in the GDPR Article 9(1). It means that the lawmaker also treats the FRT biometric practice as lawful since he mentioned article in para 2 point (a) assures the consent to be a ground allowing biometric data processing by FRT of those personal data proportionally to those that prohibited under para 1 such as biometrics, except where Union or Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject. At the

[13] GDPR, art. 4(14) states: "biometric data means personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopy data."

same time, Danish Data Protection Act in Chapter 3 stipulates that the prohibition covered by GDPR Article 9(1) does not apply in cases where the conditions for processing personal data set out in Article 9(2)(a) are met. Accordingly, for the execution of the GDPR Articles 6(1)(a) and 9(2)(a), the consent shall be regarded in means of Article 4(11)[14] as a transparent, and specific expression of the individual's wishes and voluntary will to allow personal data processing of that individual respectively. The data subject, besides the awareness about the processing, is foreseen to give unambiguous agreement through a statement or affirmative action. Also, Article 7 indicates four conditions that shall meet consent.[15]

Furthermore, it is vital to comprehend of type of data FRT at the fitness center is working with for precise customer consent to that informed special category of data. It is because entities have to comply with the data minimization principle,

---

14 GDPR, art. 4(11) states: "'consent' of the data subject means an any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by evident affirmative action, signifies agreement to the processing of personal data relating to him or her."

15 GDPR, art. 7 states: "1. Where the processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration that also concerns other matters, the request for consent shall be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration that constitutes an infringement of this Regulation shall not be binding; 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

which requires that only the necessary information be processed, and not all information available to the entities.[16] Regardless, the research has shown, that facial scanning is used to process personal data in the form of images to uniquely identify an individual falling under the meaning of the GDPR Article 4(14). In the case study about FysioDanmark a fitness center has implemented an FRT whereby a camera placed at the entrance in real time scans customers' faces unique characteristics and compares the results with data images already uploaded to the FRT database. The reliability of the tools used depends on the effectiveness of the algorithm. This effectiveness relies on different factors, such as false positives, false negatives, performance in different lights, reliability when faces are turned away from the camera, or the impact of face coverings.[17] This process involves comparison techniques with prior stored biometric templates, and results in one or more matching processes. According to the mentioned arguments, the DDPA is eligible to issue FysioDanmark with a warning that FysioDanmark processes biometric data for the purpose of uniquely identifying a data subject (customer) without obtaining consent from the person concerned under the GDPR Article 9(2)(a) is forbidden.

Applying mentioned FRT approach, the fitness center not only uniquely distinguishes individuals but also amasses information on the duration of a customer's visit by detecting their entry and exit time, and including the sum of the time customers spend in the fitness center. Significantly, the DDPA concurs with FysioDanmark that time management of entry/exit variety as well as the duration of a customer's stay are a piece of information with permitted processing if the party in question complies with the GDPR Article 6. However, the authors point out, that this type of derived data obtained through the FRT in question is interfere

16 COUNCIL OF EUR., GUIDELINES ON FACIAL RECOGNITION, *supra* note 5, at 21.

17 *Id*. at 16.

with privacy. Regardless of that, the Directive on Privacy and Electronic Communications preceded originally a necessity and ban to storage or other species of interference by bodies other than users, without the consent of the users affected.[18] In this context, the DDPA has emphasized the importance of the consent form's design and content.

Therefore, the customer's consent has to be obtained for the processing of biometric data about him or her in connection with conducting access control of customers and keeping statistics on how long customers stay in the fitness center. In this junction, consent is not assumed to be given voluntarily if the procedure for obtaining consent and design does not allow the data subject to choose appropriate variations meaning to have the possibility to give separate consent up to differentiative processing activities concerning personal data; otherwise, the consent is forced to agree with all purposes. The consent form is urged to be divided up, and the data controller must offer the data subject the opportunity to consent for one purpose but not all together. In practical terms, this can be done, for example, in the form of a comprehensive declaration where the data subject can mark by bonding "x" or alike spot about which purposes he/she acquiesces to the processing of data. Moreover, entities using FRT for identification or verification purposes have to ensure that the products or services they are using are designed to process biometric data in compliance with the principles of purpose limitation, data minimization, and limitation of the duration of storage, and integrate all other necessary safeguards into the technologies.[19]

---

18 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37, 43.

19 COUNCIL OF EUR., GUIDELINES ON FACIAL RECOGNITION, *supra* note 5, at 25.

2.1.2 Access Control Solution at the Fitness Center for Employees

The FysioDanmark has stated that employees are also offered to use facial recognition as an admission control solution and that this is used if the employee consents to this. Again, it is also a case of biometric data purpose determination to uniquely identify a natural person (employee) that is forbidden to process unless an exception to this prohibition can be identified in the GDPR Article 9(2) which stipulates the possibility of escape from the banning rule concerning working staff under the point (b). Based on that and taking into account the application of point (a) by FysioDanmark to its employees, the authors cannot agree that the employee's means of the GDPR Article 9(2)(a) can be practiced instead of point (b) unless at FysioDanmark practiced bring-your-own-device (BYOD)[20] policy when it is necessary to request employees explicit approval for device monitoring, particularly in scenarios where the employer permits the private use of company-owned devices and where the vocation employs the employee-owned device for professional tasks respectively. It is because terminal equipment of users of electronic communications networks and any information stored on such equipment *are part of the private sphere of the users* requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms.[21] And, so-called spyware, web bugs, hidden identifiers, and other similar devices can enter the user's terminal without their knowledge to gain access to information, store hidden information, or trace the activities of the user *and may*

---

20 To understand the concept of BYOD, *see e.g.*, BOB HAYES & KATHLEEN KOTWICA, BRING YOUR OWN DEVICE (BYOD) TO WORK: TREND REPORT (2013).

21 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37, 39.

seriously intrude upon the privacy of these users.[22] At the same time, the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity[23] and thus with no connection to a professional or commercial activity.[24] Yet, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities. Furthermore, in most Member States, such as the Netherlands, Germany, and Italy employers are not authorized to use biometrics for the time and attendance senses even on the ground of point (b).[25]

The employee's consent within the meaning of point (a) shall not form the basis at FysioDanmark for facial unique data processing because:

i. there is an unequal relationship between the data controller and the data subject "in the context of relationships such as employer-employee."[26] In that esteem, the worker is regarded as the weaker party, and "it is, therefore, necessary to prevent the employer from being in a position to impose a fetter of employee rights on him"[27] due to the imbalance of power that can exist between the parties involved;

---

22 *Id*.

23 Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.

24 GDPR, Recital 18.

25 *See* Daria Bulgakova, *Case Study on the Fingerprint Processing in a Workplace Under GDPR Article 9 (2, b)*, 124 TEISĖ 22, 24 (2022).

26 Moira Paterson & Maeve McDonagh, *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*, 44 MONASH U. L. REV. 1, 14 (2018).

27 Case C-55/18, Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE, ECLI:EU:C:2019:402, ¶ 44 (May 14, 2019); also *see*, C-397/01 to C-403/01, Bernhard Pfeiffer and Others v Deutsches Rotes Kreuz, Kreisverband Waldshut eV, EU:C:2004:584, ¶ 82 (Oct. 5, 2004); C-429/09, Günter Fuß v Stadt Halle, EU:C:2010:717, ¶ 80 (Nov. 25, 2010); C-684/16, Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. v Tetsuji Shimizu, EU:C:2018:874, ¶ 41 (Nov. 6, 2018).

ii. on account of the position of weakness, a worker may be dissuaded from explicitly claiming his rights vis-à-vis his employer where, in particular, doing so may expose him to measures taken by the employer likely to affect the employment relationship in a manner detrimental to that worker;[28]

iii. on the other side, according to the GDPR Recital 40, in order for processing to be lawful, personal data *should be processed on the basis of the consent* of the data subject concerned or *some other legitimate basis, laid down by law*, including the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. But, recitals consider the following reasons for the articles of the GDPR, and if the article answers the query "what?", the recital provides additional knowledge about "when?" and "how?". The articles are binding, but recitals are not. Thus, referring to the above arguments about unbalanced employment relationships, in the authors' view, the employment contract could not be a legitimate basis in the scenario of the FysioDanmark case study since its force overweight the right to personal data protection of an employee with respect to fundamental human rights law and would cause biometric data processing against of an employee "will" with respect to human dignity and human-centric approach in the EU. Respectively, Wojciech Wiewiórowski highlights the importance of the precautionary principle, which may even justify a ban or temporary freeze on some uses of the technology where its impact on society and the rights and freedoms

28 *See Fuß*, C-429/09, EU:C:2010:717, ¶ 81; *Max-Planck-Gesellschaft*, C-684/16, EU:C:2018:874, ¶ 41.

of individuals is uncertain;[29]

iv. once the infrastructure is in place, FRT may be at hand for "function creep". Moreover, poor-quality underlying datasets can result in bias or discrimination; correcting such biases is often a task that is outsourced, so the wider human impact also needs to be considered.[30] Also, – according to Article 6 of the Directive 89/391/EEC[31] the employer's obligation is within the context of his responsibilities to take the measures necessary for the safety and health protection of workers, including prevention of occupational risks implementing the measures on the basis of the following general principles of prevention: (a) avoiding risks; (b) evaluating the risks which cannot be avoided; (c) combating the risks at source; (e) adapting to technical progress; (f) replacing the dangerous by the non-dangerous or the less dangerous; (g) developing a coherent overall prevention policy which covers technology, organization of work, working conditions, social relationships and the influence of factors related to the working environment, – having regard to the essential objective pursued by Directive 2003/88,[32] which is to ensure the effective protection of the living and working conditions of workers and better protection of their safety and health, they are required to ensure that the effectiveness of

29 Wojciech Wiewiórowski, *AI and Facial Recognition: Challenges and Opportunities*, EUR. DATA PROT. SUPERVISOR (Feb. 21, 2020), https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en.

30 *Id*.

31 Council Directive 89/391/EEC of 12 June 1989 on the Introduction of Measures to Encourage Improvements in the Safety and Health of Workers at Work, 1989 O.J. (L 183) 1, 1-8.

32 Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 Concerning Certain Aspects of the Organization of Working Time, 2003 O.J. (L 299) 9, 9-19.

those rights is guaranteed in full.[33] Thus, employers should ensure the safety and health of their workers by evaluating and mitigating risks associated with FRT. It is rational that biometric data processing directly depends on machine employment.[34] The underlying datasets used in FRT can be biased, leading to unfair treatment of employees and an unhealthy working environment. Biometric data processing includes complicated, complex algorithms when processed data can be transformed and fragmented several times.[35] Therefore, safe well-being at the workplace shall be at first place against the unjustified employment of biometric technology and keep respect for the biological nature of human origin.

The four arguments specified above demonstrate the amount of incompatible biometric FRT experience at the workplace due to the contradictory interests of both parties.[36]

---

33 Case C-55/18, Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE, ECLI:EU:C:2019:402, ¶ 42 (May 14, 2019).

34 Daria Bulgakova, *Unique Human Identification Under the GDPR Article 9 (1) (2)*, 1 PHIL. L. & GEN. THEORY L. 130, 154 (2022).

35 *Id*. at 155.

36 Notably, also according to the European Data Protection Board (EDPB), Guidelines 3/2019 on Processing Personal Data Through Video Devices, version 2.0, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and On the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2020, 47, at 14. Given the imbalance of power between employers and employees, in most cases employers should not rely on consent when processing personal data, as it is unlikely to be freely given. For example, Data Protection Authority in the Netherlands in a case about Windows 10 operating system (2017) assumes that the developer could not rely on the legal grounds necessary for legitimate interest or the performance of an agreement because (i) it infringes the Telecommunications Act by not obtaining consent prior to the collection of the data; (ii) it processes the data for different purposes and has not demarcated what data it processes for each of those purposes, and (iii) the interest of the developer in processing sensitive data does not

A FysioDanmark has explained that if an employee does not wish to use the system, he or she can instead use a physical access card and password.[37] Furthermore, the DDPA assumes that the system only registers data about the employee in connection with his or her access to the fitness center, and no data is recorded about the employee's movements in the center in general.

Accordingly, the research offers a specific assessment cited as follows. Whether, and to what extent, it is necessary to set up a system enabling the duration of time worked each day by each worker to be measured in order to ensure effective compliance with maximum weekly working time and minimum daily and weekly rest periods must be examined in the light of those general considerations.[38] On the other hand, in the absence of such a system, there can be no guarantee that the time limitations laid down by Directive 2003/88 will actually be observed or, consequently, that the rights that the directive confers on workers may be exercised without hindrance.[39] Indeed, in the absence of any system for

---

outweigh the right to protection of the private life of users. *Available at*: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/public_version_dutch_dpa_informal_translation_summary_of_investigation_report.pdf (last visited Jan. 1, 2023).

37 The Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) made an injunction order against Sportitalia, an amateur sports club with limited liability, fined a sports club €20,000 for uncompliant a fingerprint system to record the attendance of its workers (2022).
Case 9832838, Garante per la protezione dei dati personali (Italy) v. Sportitalia (the controller), No. 369 (Nov. 10, 2022), https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9832838.

38 Case C-55/18, Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE, ECLI:EU:C:2019:402, ¶ 46 (May 14, 2019).

39 Advocate General Pitruzzella (Opinion of the Case C-55/18, Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE, ECLI:EU:C:2019:402), regardless of Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE, Case

measuring working time, there can be no way of establishing objectively and with certainty how much work has actually been done or precisely when it was done. Moreover, without such a system, it will not be possible to differentiate between ordinary working hours and overtime or, consequently, to verify with ease and certainty whether the limits introduced by Directive 2003/88 are being observed in practice.[40] In those circumstances, it appears to be excessively difficult, if not impossible in practice, for workers to ensure compliance with the rights conferred on them by Article 31(2) of the Charter and by Directive 2003/88, to actually benefit from the limitation on weekly working time and minimum daily and weekly rest periods provided for by that directive.[41] In particular, it must be emphasized that, taking into account the worker's position of weakness in the employment relationship,[42] by contrast, a system enabling the time worked by workers each day to be measured offers those workers a particularly effective means of easily accessing objective and reliable data as regards the duration of time actually worked by them and is thus capable of facilitating both the proof by those workers of a breach of the rights conferred on them by Articles 3 and 5 and 6(b) of Directive 2003/88, which give specific form to the fundamental right enshrined in Article 31(2) of the Charter and also the verification by the competent authorities and national courts of the actual observance of those rights.[43] Consequently, in order to provide the effectiveness of those rights provided for in Directive 2003/88 and of the fundamental right enshrined in Article 31(2) of the Charter, the Member

C-55/18, ECLI:EU:C:2019:87, about Health and Safety of Workers in the Workplace & Obligation for Undertakings to Set up a System to Measure Daily Working Time, ¶ 57 (Jan. 31, 2019).

40 *Id*. ¶ 58.

41 Case C-55/18, Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE, ECLI:EU:C:2019:402, ¶ 48 (May 14, 2019).

42 *Id*. at ¶ 55.

43 *Id*. at ¶ 56.

States must require employers to set up an objective, reliable and accessible system enabling the duration of time worked each day by each worker to be measured.[44]

Thus, the research, besides of inappropriateness of the GDPR Article 9(2)(a) application in employment relationships, also emphasizes the importance of having an objective, reliable, and smoothly accessible system to accurately measure and record working time where in the authors view, the FRT to uniquely recognize the employee facial data is not a justifiable method unless such a procedure would provide workers with trustworthy securities against any breaches of their rights with an affiliated flag by relevant authorities that verify compliance.

3. RESEARCH RESULTS

Consent is a regulatory tool to secure proportionality and is word-for-word linked to the primary purpose of biometric data processing. Hence, the study criticizes the lack of definite criteria in GDPR regarding the legitimate interests concerned.[45] Also, regarding any terminal device matter, the human-centric approach[46] indicates that if the data is stored on such an apparatus, then a person shall control it. Furthermore, based on the Directive 93/13/EEC,[47] a document of a per-formulated consent (by the controller) should be administered in an understandable and undoubtedly easy form, applying definite expression, and

44 *Id*. at ¶ 60.

45 For example, in DPC Report at Case Study No. 6 (2011) the Data Protection Commissioner in Ireland determined the processing of biometric data of customers purchased for a car dealership. In these cases, customer data can be legitimately used if it is for the same purposes as the previous owner had used them. *Available at*: https://www.dataprotection.ie/documents/annualreports/AnnualReport2011.pdf (last visited Mar. 1, 2023).

46 *See* LÉONCE BEKEMANS, GLOBALISATION VS EUROPEANISATION: A HUMAN-CENTRIC INTERACTION (2013).

47 Council Directive 93/13/EEC, of 5 April 1993 on Unfair Terms in Consumer Contracts, 1993 O.J. (L 95) 29, 29-34.

should not restrain unfair phrases.[48]

Unlike other non-special categories of personal data, there is a risk of unique identity being used for secondary purposes as soon as the biometric data processing is completed and continues to be stored in the database. Thus, the research is deemed as a matter of the principle of proportionality application through the lawful basis to achieve the aim of unique identification that found itself on the consent.[49] Consent should not be deemed as freely granted if the biometric data subject has no known or has no free choice either is weak to reject or revoke consent without detriment.[50]

3.1 Video Surveillance in the FysioDanmark Case

Based on the case materials, the camera installed at FysioDanmark's entrance is constantly connected to the internet, and FRT does not require any additional activation steps, such as keystrokes, to start functioning. As a result, the camera, along with the FRT it contains, remains active and captures data also about those individuals (prospective customers and/or visitors) who randomly came and when they enter the FRT field of view. However, the FysioDanmark has clarified that if an individual chooses not to partake in facial recognition, their facial unique data is not operated for facial recognition purposes unless it has been previously stored in the FRT system.

The research has shown a distinguishing feature of the collection, use, and disclosure limitation principles is that they are not, in the main, based on a consent model.[51] Taking into account that the consent idea at the FysioDanmark is implemented together with the membership privilege, it means for the research that

48 *Id*. at 29.
49 GDPR, Recital 40.
50 GDPR, Recital 42.
51 Paterson & McDonagh, *supra* note 26, at 13.

the *newly came prospective customers and/or visitors have not been asking and/or could not be asking* about FRT use to their faces, *and logically those people facial data would not be stored in the FRT system*. Despite this limitation, the FRT pursuit is to uniquely identify activities within the appropriate camera range for everyone entering the premises, meaning that the unique identification purpose would not be achievable regardless of the incomplete or unsuccessful process because the prospective customers and/or visitors "new" faces do not match any facial image in the FRT memory as it's had trouble due to the processing hardship. Accordingly, *the FRT is vigorously working over anyone's facial unique data from the moment when individuals enter the range of the FRT camera meaning that the process of unique identification begins*. Nevertheless, due to incompatibility with the faces in the system or an inability to find a match, the process may yield a negative output or be rejected. Therefore, *the FRT system remains active in processing the video feed of individuals within its range*; hence, in such scenarios, the practice of FRT can be analogized to regular video surveillance.

The emphasis here is not on the outcome of planned unique identification but rather *on the ongoing processing and trials of FRT to finalize action to uniquely identify*. As an effect, the complete and accurate identification of newly arriving individuals *cannot be achieved through* the qualitative matching of their faces against the stored database. It also implies that based on the principle of data accuracy[52] the controller should not use data without taking steps to ensure with

52 GDPR, art. 5(1)(d). *See*, for instance, also the implementation of the data accuracy principle in Belgium, Act on the protection of private life regarding the processing of personal data (Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel/Wet tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens), art. 4(1)(4), 1992; Spain, Organic Law 15/1999, of 13 December 1999, on Protection of Personal Data (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal), art. 4(5), 1999.

reasonable certainty that the data are accurate and up to date otherwise inaccurate personal data shall be erased or rectified without delay. Hence, fitness centers *should refrain from using FRT on individuals who have not given their consent, even if their facial data is not stored in the FRT database*. This is because the system's *performance is inherently inaccurate* and cannot successfully complete the operation of unique identification. The unreliable and imprecise data provided by the system makes it impractical to rely on FRT for unique identification purposes. According to public officials that FRA interviewed, the use of electronic readers to minimize manual entries, as well as automatic verification against other data entries, when applicable, could contribute to reducing the risk of mistakes.[53] The FRA research indicates that the quality of data could be strengthened if the authorities increasingly involved the person concerned in the verification procedures, and if they were open to plausible arguments that the person concerned presents.[54]

The DDPA assessing the video surveillance situation at FysioDanmark terminates that *biometric data is processed* for the purpose of unique identification of persons *who have not consented* to such a method. This is because, according to the wording of Article 9(1), it is the very purpose of the processing – *of uniquely identifying* the data subject(s) using biometric data – that determines whether the processing falls within the banning scope. *It is*, therefore, *immaterial whether a match occurs or whether there is actually a full unique identification or a finality of the purpose is completed*. Thus, wherever biometric data processing is based on the person's approval, the company should demonstrate that it is given correspondingly to the factual processing performance. In particular, the meaning

53 FRA, *supra* note 6, at 88.

54 *Id*. at 97.

of a signed confirmation, safeguards though the burden of proof[55] should guarantee that the data subject is knowledgeable of the fact itself and the degree of permission shall be clarified too. This is also the case when the treatment has quite a volatile (short-term) nature. Besides, the FRT at FysioDanmark is installed in a controlled environment by the fitness center respectively, and that party should prevent third parties be at risk. In this context, the controller should consider physical and technical means, for example blocking out or pixelating not relevant areas.[56] At the same time, in contrast to an uncontrolled environment, which means that the system involves capturing on the fly the faces of any individual passing in the range of the camera, including persons who have not consented to the biometric device, thereby creating biometric templates.[57] These templates are compared to the ones created of data subjects having given their prior consent during an enlistment process (i.e., a biometric appliance user) in order for the data controller to recognize whether the person is a biometric device user or not.[58] In

55 *See* the EDPB Guidelines 3/2019, at 11, questions concerning the processing's necessity also arise regarding the way evidence is preserved. In some subjects, it might be necessary to use black box solutions where the footage is automatically deleted after a certain storage period and only accessed in case of an incident. In other situations, it might not be necessary to record the video material at all but more appropriate to use real-time monitoring instead. The decision between black box solutions and real-time monitoring should also be based on the purpose pursued. If for illustration, the purpose of video surveillance is the preservation of evidence, real-time methods are usually not suitable. Sometimes real-time monitoring may also be more intrusive than storing and automatically deleting material after a limited timeframe. The data minimization principle must be regarded in this context (Article 5(1)(c)). It should also be kept in mind that it might be possible that the controller could use security personnel instead of video surveillance that are able to react and intervene immediately.

56 EDPB, Guidelines 3/2019, at 11.

57 *Id*. at 20.

58 *Id*.

this case, the system is often designed to discriminate the individuals it wants to recognize from a database from those who are not enlisted.[59] Consequently, people can only use described way of video surveillance which entangles biometrics functionalities if there is explicitly informed consent (according to the GDPR Article 9(2)(a)) beforehand. However, in order to ensure that no one who has not previously given his or her consent is captured, *the FRT biometric method is advised to be triggered by the data subject himself, for instance by pushing a button*. To ensure the lawfulness of the processing, *the controller must always offer* an alternative way to access the building, without biometric processing.

Notably, the use of *video surveillance including biometric recognition* functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, *require explicit consent from all* data subjects (Article 9(2)(a)), however, another suitable exception in Article 9 could also be applicable.[60] On the other hand, *the processing of photographs* should not systematically be considered to be a processing of special classifications of personal data as they are *covered by the definition of biometric data only* when processed through a *specific technical means allowing the unique identification* or authentication of a natural person.[61]

---

59 *Id*. For example, a hotel uses video surveillance to automatically alert the hotel manager that a VIP has arrived when the face of the guest is recognized. These VIPs have priory given their explicit consent to the use of facial recognition before being recorded in a database established for that purpose. These processing systems of biometric data would be unlawful unless all other guests monitored (in order to identify the VIPs) have consented to the processing according to Article 9(2)(a) GDPR.

60 *Id*. at 18.

61 GDPR, Recital 51.

4. CASE STUDY FINALITIES

4.1 Outcome in the FysioDanmark Case

In its decision, the DDPA only considered whether GDPR Article 9(1) and 9(2)(a) serves with respect to Article 6 as the legal basis for the processing and did not address other data protection law issues. *The DDPA issued a cautionary notice* to a company regarding its raised use of an FRT to uniquely identify. According to the DDPA, the FRT could only process biometric data in this manner with the explicit consent of the data subjects, as stipulated under Article 9(2)(a) of the GDPR. Therefore, the DDPA has cautioned that otherwise founded practice would be a violation as no exceptions are realized under para 2. As a result, referring to the given power in the GDPR Article 58(2), the DDPA issued the warning for FysioDanmark. It means FysioDanmark must take the necessary steps to comply with the warning. As part of its advisory role, *the DDPA suggests exploring options for implementing the FRT in a route that guides a person to activate the plan on his own at first hand (such as through keystrokes) for the execution of a consent that the individual signed for neither broadly nor continuously run the system.* This scheme could confirm and assure that the unique identification was demanded only for those who consented.

In the study's opinion, the question of representing a person through biometrically digitized human characteristics must be placed in the context of legitimate interest. Processors shall legally convince a precise customer to trust and mitigated risks to natural human characteristics. It is appropriate when individuals would like to receive approval about the safeness of FRT practice due to legitimate anticipations on specific protection. Hence, *balancing claims is mandatory*.[62]

62 EDPB, Guidelines 3/2019, at 11.

Fundamental rights and freedoms on the one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully.[63]

4.2 Conclusions

Consent remains a crucial aspect, and it is important to ensure that it is obtained effectively. The research clearly indicates that facial recognition involves special categories of data, specifically biometrics. Private players have the responsibility to understand their specific obligations under applicable legislation. They are also in the best position to come up with innovative and creative solutions for establishing a consent process that aligns with the GDPR and the nature of their relationship with customers and employees. There are no prescribed formats related to consent to give prominence, and obtaining compliant consent from those whose biometric data is being processed is crucial to establish a legitimate basis for the services provided and the handling of personal data.

In the context under consideration, when explicit consent from the individuals concerned is not obtained, it creates a situation where both the company and the individuals lack the equal capacity to negotiate the consequences of consent. This leads to the inability to access places and can result in discriminatory effects that undermine human dignity. Therefore, it is vital thoroughly assess certain aspects, including the nature and source of the data, its implementation process, and, most importantly, the purpose for which it is utilized to confirm the authorization and

63 *Id*. For example, a private parking company has documented reoccurring problems with thefts in the cars parked. The parking area is an open space and can be easily accessed by anyone but is clearly marked with signs and road blockers surrounding the space. The parking company has a legitimate interest (preventing thefts in the customer's cars) to monitor the area during the time of day that they are experiencing problems. Data subjects are monitored in a limited timeframe, they are not in the area for recreational purposes, and it is also in their own interest that thefts are prevented. The interest of the data subjects not to be monitored is in this case overridden by the controller's legitimate interest.

legality of facial label practices. These elements should be examined in conjunction with the principles outlined in the GDPR and determined if the extents implemented are proportionate to the intrusion into the data protection right of the individuals concerned, as defined in Article 52(1) of the Charter of Fundamental Rights of the European Union. Furthermore, the strike about the balance of legitimate interests to any treatment involving unique identification in the private sphere must adhere to the principle of proportionality considering the accompanying conditions and safeguards in place to mitigate potential adverse outcomes as justified and appropriate.

The production of biometric FRT and its further installation in the private sector has to be governed from the side of prohibition to force individuals to assent the unique identification and to avoid the placement of the person on unequal uncomfortable relationships for sufficient application of the GDPR Article 9(2)(a). Through this bid, the GDPR Article 9 para 2(a) basis in the employment relationships creates doubts when interpreting its rationale. The level of intrusion must possess the principle of proportionality assessment, which, according to the studied legislation, requires the expression of the freely given consent of the data subjects (employees). It is not freely given as in the studied case about employee consent, then this must be corrected with the support of another basis to exempt from para 1 strong enough to justify the unique identification cure to obtain the desired purposes and demonstrate for the worker concerned safeguards such as the maintenance of the proper functioning of the prevention of theft.

The dedicated regulatory framework still needs to be improved regarding the enforcement of FRT and appropriate lawful use.[64] The research recommends

64 *Id*. at 7, 9. Significantly, as per EDPB Guidelines 3/2019 in the event of FRT practice for video surveillance based on the mere purpose of "safety" or "for your safety is not sufficiently specific" (Article 5(1)(b)). It is furthermore contrary to the principle that personal data shall be processed lawfully, fairly, and in a transparent manner in relation to

approving a standard with rank of law that justifies explicitly to what extent and what assumptions the use of FRT with biometric systems would respond to an obedient application as best practices evolving across different sectors in the future to guarantee that the consent details are effectively conveyed, and additional emphasis may be necessary in certain cases.

5. RECOMMENDATIONS

Right holders are frequently not fully familiarized with biometric data processing producing troubles assuming the notice they receive as appropriate. The criterion of consent as a means of balancing interests is criticized since even if permission is given, and as soon as tech progress imminently accommodates various projects, that will continually interface with risks to humans. In this regard, the research recommends realizing the right to personal data protection means of dignity prioritization and shielding the human body against its over-execution. It is because, in the assertion of the breakdown, the implementation of the biometric technology does not serve as a significant way to practice nor poses risks to the human integrity of each individual when the last shall prevail in any scenario.

Therefore, private players should prioritize providing individuals with upfront access to key elements that impact their decisions. Thus, a consent shall enclose:

- ✓ Clearly expressing what personal data;
- ✓ Transparently pointing with which parties the personal data might be intercommunicated;
- ✓ Undoubtedly wording the purposes for personal data processing;

---

the data subject (see Article 5(1)(a)). Furthermore, the GDPR is not applicable to fake cameras (i.e., any camera that is not functioning as a camera and thereby is not processing any personal data). However, in some Member States, it might be subject to other legislation.

- ✓ Telling individuals about the potential risks of harm and other influences associated with data processing.

Institutions should submit these details in manageable and easily obtainable modes, qualifying individuals to maintain the level of detail they expect to get because people may have varying preferences for the amount of information they review as well as the timing of their consent findings. Therefore, institutions should respect and sustain different practices, such as presenting information in a layered format or providing summaries of key highlights upfront. Furthermore, the consent extract should not be a one-time conclusion. Individuals should have the ability to rethink and shrink their consent at any time, with full reports readily obtainable to defend their decisions. Interactive walkthroughs, videos, infographics, and other visual tools can benefit. The institution will show user-friendly consent processes by following these recommendations as per the research expectations.

References

Books

BEKEMANS, LÉONCE, GLOBALISATION VS EUROPEANISATION: A HUMAN-CENTRIC INTERACTION (2013).

HAYES, BOB & KATHLEEN KOTWICA, BRING YOUR OWN DEVICE (BYOD) TO WORK: TREND REPORT (2013).

Journals

Bulgakova, Daria, *Case Study on the Fingerprint Processing in a Workplace Under GDPR Article 9 (2, b)*, 124 TEISĖ 22 (2022).

Bulgakova, Daria, *Unique Human Identification Under the GDPR Article 9 (1) (2)*, 1 PHIL. L. & GEN. THEORY L. 130 (2022).

Paterson, Moira & Maeve McDonagh, *Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data*, 44 MONASH U. L. REV. 1 (2018).

Other Resources

AZRIA, SANDRA & FRÉDÉRIC WICKERT, CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (CONV. 108), COUNCIL OF EUR., FACIAL RECOGNITION: CURRENT SITUATION AND CHALLENGES (2019), https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1.

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (CONV. 108), COUNCIL OF EUR., GUIDELINES ON FACIAL RECOGNITION (2021), https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.pdf.

European Data Protection Board (EDPB), Guidelines 3/2019 on Processing Personal Data Through Video Devices, version 2.0, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and On the Free Movement of Such Data, and Repealing Directive

95/46/EC, 2020.

EUR. UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), UNDER WATCHFUL EYES: BIOMETRICS, EU IT SYSTEMS AND FUNDAMENTAL RIGHTS (2018), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf.

MADIEGA, TAMBIAMA & HENDRIK MILDEBRATH, EUR. PARL. RSCH. SERV., REGULATING FACIAL RECOGNITION IN THE EU (2021), https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf.

Wiewiórowski, Wojciech, *AI and Facial Recognition: Challenges and Opportunities*, EUR. DATA PROT. SUPERVISOR (Feb. 21, 2020), https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en.