GDPR in access control and time and attendance systems using biometric data

Goran Vojković, Ph.D.
Melita Milenković, LL.M.

University of Zagreb
Faculty of Transport and Traffic Sciences
Vukelićeva 4, Zagreb, Croatia
E-mail: goran.vojkovic@fpz.hr
melita.milenkovic@fpz.hr

Abstract – The new General Data Protection Regulation (GDPR) begins to fully apply on May 25, 2018, and EU Member States have to transpose it into their national law by 6 May 2018. By this Regulation (i.e. by a binding act directly applicable), the European Union regulates the questions of personal data protection in a significantly different and more up-to-date way than regulated by the previous regulations. For the first time, biometric data, are also defined as personal data obtained by a special technical processing related to physical, physiological characteristics, or characteristics of an individual's behaviour, which provide or confirm the unique identification of the individual, such as face recognition or fingerprint identification. Given that these data are very commonly used in access control and time and attendance systems, in this paper, we would like to present the novelties that the GDPR brings, and which will have to be respected by everyone whose access control system or time and attendance systems are based on biometric data.

I. INTRODUCTION

The new General Data Protection Regulation (GDPR) [1] begins to fully apply on 25 May 2018. This is a new act that regulates the matters of personal data protection in the EU countries in a very different way. Let's remember that the first modern act relating to this area is the Convention on the Protection of Individuals regarding the automatic processing of personal data [2] of the Council of Europe (Convention 108). This is the Convention of the Council of Europe, but since all EU members are also members of the Council of Europe, the Convention has been generally applied and applies within the EU.

The Convention in force was opened for adoption on 28 January 1981, in Strasbourg, and entered into force on October 1 1985 after its fifth ratification. Despite the exceptional significance of the mentioned Convention, its provisions are partially out of date, in practice, due to the flow of time - at the time when it was written there was no high-speed internet in the present sense, there was no cloud computing, there was a lack of personal data not as nearly in the way it's done now.

The European Union has reformed the area of personal data protection in 1995 when the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3] came into force. This Directive, together with Convention 108, is the foundation for the adoption of national personal data protection laws, the establishment of national regulatory agencies and the existing personal data protection model, which has been developed by so far.

Let us also mention how some other regulations, relating to the areas of personal data protection have also been adopted e.g. in electronic communications, (but they are not essential to our paper).

Since the adoption of Directive 95/46/EC has passed many years, and it has begun to show some disadvantages, and legal practice has also shown that some standards can be regulated in a better manner. That is the reason why it all started with the adoption of a new regulation, and after a couple of years the GDPR was adopted.

Here we have to point out on another difference between the current legal framework and the GDPR. On the contrary to Convention 108 which was supposed to be fully incorporated into national regulation as an international convention, and to Directive 95/46/EC which had to be transposed into domestic acts ‘’the GDPR is a binding legislative act. It has to be applied in its entirely across the EU, while a directive is a legislative act that sets out a goal that all EU countries have to achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast to the previous legislation, which is a directive.” [4]

In this paper, we shall analyse the GDPR rules in relation to today's common collection of biometric data for the purpose of access control and time and attendance systems. GDPR explicitly defines biometric data where: “‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data” (GDPR, Article 4, and explicitly limits their application).

II. DACTYLOSCOPIC DATA

Dactyloscopy is a contemporary, safest and most widespread method of determining persons' identity, on the basis of friction ridges (friction ridges on the surface of the inside of the fingers, palms and soles of the feet). Friction ridges are formed even before birth and do not change during life, they are strictly individual (there are no two

persons with the same friction ridges). Also, fingerprints are easily classified in practice. [5] After being applied for almost a century in police and criminology in practice, the use of dactyloscopic data has become extremely popular in access control and time and attendance systems.

With the GDPR's entry into force, several important questions are being raised: can the organization use our data undisturbed? Do we have to agree to biometric identification, or are we entitled with the right to alternative? How is the organization obliged in keeping our data? In this paper, we shall try to provide answers on some of these questions, without any pretense that our conclusions are final – because we believe that legal practice within this area will be developing in years to come.

It is legitimate to ask the question of the importance of storing the dactyloscopic data. Mathematically, they should be unique to each person. As they are unique, and easy to read, it seems almost ideal in access control and time and attendance systems However, this uniqueness and easy reading can also represent a potential security risk. Today, fingerprints can be easily forged. There are even instructions on how to forge a person's fingerprints, such as on the Internet's page: "How to Fake Fingerprints?" [6]. This practice is not even illegal as long as fake fingerprints are not misused!

In a situation where there is great confidence in fingerprint identification, but which can be relatively easily forged, there is a serious security problem. What happens in the case of misuse? While the fingerprint identification is taken as common and "safe", how much time and resources will it take in cases of misuse to prove that a false fingerprint was used? We consider that the attention which the GDPR has dedicated to biometric data is therefore, quite appropriate.

III. THE EXISTING SOLUTIONS

Manufacturers of modern smartphone devices commonly use fingerprint recognition to access more expensive devices. By simply pressuring the sensor is easier than entering a code or by using a similar identification method. However, it seems they were aware of the dangers of collecting of biometric data, so they placed them on the separate chip, on the device itself. Here's an example for Apple:

"The chip in your device includes an advanced security architecture called the Secure Enclave, which was developed to protect your passcode and fingerprint data. Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data.

Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave. Your fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases." [7]

This kind of technological solution introduced years before the entry into force of GDPR can be characterized as very useful. But here it's about a well-known smartphone manufacturer who invests tremendous resources in securing the use of its devices. An omission in the field would cost a company billions of dollars.

And what about hundreds of different devices and manufacturers of various solutions for access control and time and attendance systems? What kind of security systems do they have and what do we have to look for from them? First of all, to answer these questions, first we have to analyse the provisions of GDPR on the protection of biometric data.

IV. GDPRG AND BIOMETRIC DATA

The processing of biometric data is defined by the Art. 9 of the Regulation, under the title "Processing of special categories of personal data", therefore, among the data that must be additionally protected, as emphasized in the paragraph 53 of the Preamble of the Regulation: "Special categories of personal data which merit higher protection". It gives an additional responsibility for processing and storage of biometric data.

The basic provision is that processing of such data is not permitted (Art. 9, Para 1): "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, shall be prohibited for biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Subsequently, (Para. 2) lists an entire range of exceptions, which we fully quote: "Para. 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental

rights and the interests of the data subject; (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

Due to its importance, we also list the remaining two paragraphs:

''3. Personal data referred to in Para. 1 may be processed for the purposes referred to in point (h) of Para. 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person shall also be subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."

Therefore, Member States may introduce stricter regulation of this category of data.

When we analyse a very extensive article with a large number of exceptions – it's immediately apparent that the most of them are related to the collection of biometric data for the needs of different states, or for health purposes. Only a few of the provisions can be applied for the purposes of this paper - access control and time and attendance systems.

V. BIOMETRIC DATA IN CORPORATIVE ENVIRONMENT

As a model for the purpose of this paper, we used a company with time and attendance system based on biometric data but also an information security system ISO/IEC 27001 [8], which provides additional fingerprint identification used in access control systems when entering the server room [9] as a specially protected area.

If we look closer to the provisions of the Regulation, in such a corporate environment, only Para. 9. Art. 2. (a) and (b) can be used. The case where an employee or associate who should be allowed to access control system, gives permission for use of their own biometric data, specifically, in this case fingerprints, is quite simple. In Para. 9. Art. 2 (a) of the Regulation it's stated: "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes". So, if the employee explicitly authorizes the use of their fingerprints for access control to control their working hours (explicit approval should then be interpreted as a written approval) - then there is no obstacle to collect their biometric data.

The problem arises if an employee refuses to sign such an approval or withdraws an approval which has already been given. Art. 7 Para. 3 of the Regulation specifically states: "The data subject shall have the right to withdraw his or her consent at any time." And what happens then? The company no longer has the right to use biometric data, here fingerprints, and cannot force an employee to give them permission, nor can punish them, if he/she withdraws their approval. Nor can bind a work relationship with a consent in the sense of this provision, because it explicitly states: voluntary consent. The sanctioning of employees for non-compliance of a voluntary consent is not acceptable, and the dispute related to such a sanction would probably not be favourable for the employer. That leaves us with the provision of the Article 2, para. 9, (b), '' processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

It's hereby stated that the processing of biometric data is allowed for the purposes of the labour law, and time and attendance systems belong in this category. However, then it should be defined by the particular regulations, or by the collective agreement.

Consolidated Version of the Treaty on the Functioning of the European Union [10] Art. 288 states: "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States." In addition, the literature states that the "Member States and their national bodies are banned from interpreting of the Regulation, as well as the modification of its content". [11]

However, when the Regulation states that a national regulation may elaborate or otherwise amend its provisions, then a national state may do so. It's particularly interesting the provision on the processing of biometric data, and it can be regulated by a collective agreement. In that case, if control of time and attendance system is allowed by using fingerprints, either by national regulation or by a collective agreement, is allowed, this could become binding for the employees. The employees could express doubts and request for surveillance if they consider that the safety protection of their biometric data are not fulfilled.

Specifically, the arrangement of biometric data collection for the purpose of time and attendance system on the national level, by regulations or by collective agreement naturally applies only to that country - but in case of multinational corporations the problems might occur - each EU country may have this issue differently resolved or not to have a solution at all, if it has not introduced the national regulation.

Furthermore, this solves only the question of time control, but what happens to the access control system inside the facility, where control is allowed or identified on biometric data? Labour law does not speak of it for it does not enter the work processes. In case that an employee refuses to provide their biometric data, it's possible that in

the dispute, court may stand aside the employee, taking into account that there is possible other way of access control systems, e.g. by entering an access password. There is still no case law of European Court of Justice, but who would be ready for 2-3 years of trial, whereby strong trade unions will surely stand on the side of employees. Access control system and time and attendance system by using biometric data, specifically fingerprints is widespread all around the world. By entering into force by the GDPR – such method of identification can in large measure be in question. How will the GDPR development continue on national levels, and even within collective agreements – for now it's far too early to predict.

Let us also mention a view of the literature (about Directive 95/46/EC): "Sensitive personal data may be processed to comply with employment law obligations, whether such law derives from statute or court or tribunal precedent and whether such processing is carried out by an employer or anyone else. It is highily unlikely that the phrase 'imposed by law' could be taken to include contractual obligations – an employer will thus be unable to legitimize sensitive personal data processing by including a relevant provision in the employment contract." [12]

VI. BIOMETRIC DATA IN GOVERNMENT ENVIRONMENT

Both the state-owned companies and the civil services will face the same challenges, same as the private companies, mentioned in the previous chapter. However, when processing classified data, we consider that the provision of the Article 9, Para 2 (g) may apply, and it states: "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

Classified data can be considered as data protected for the sake of public interest (which is in the definition of classified information, and corporate and private data are protected by the business secrets). Therefore, it is considered that persons who have access to such data may be required to accept biometric verification or biometric data as part of their duties. That is to say, for a degree of secrecy (TOP SECRET, SECRET, CONFIDENTAL) they should undergo security checks and receive the appropriate certificate, at least that is the case in Croatian legislation. [13]

VII. CONCLUSION

Several authors have already noticed how the GDPR has put biometric data into a special, sensitive group. For example, Ross states: "As the GDPR considers biometric data to be a special category of sensitive personal data, processing and protecting it must proceed under the framework reserved for sensitive personal data generally. While the GDPR broadly prohibits the processing of sensitive personal data, it recognizes certain bases to justify its processing, chiefly, the explicit consent of the data subject, the performance of specific contracts or processing for certain specific purposes." [14] An interesting observation is also made by Bailey: "Because the EU member states have not been able to reach a clear consensus about the use of biometric data, however, the legal requirements applicable to the use of biometrics can still vary between the member states. This means that the GDPR cannot entirely live up to its promise of completing the internal market by fully harmonising the requirements applicable to the processing of personal data, at least where the processing of biometric data is concerned." [15] We find similarity in the other documents and analyses, for example: "Using biometrics for access control in the workspace, such as facial, iris, or finger print scanners, appears problematic as well, as employers cannot rely on consent, and no other exception to the general prohibition to process biometric data appears applicable. Member states are permitted to create their own rules concerning biometric data, however." [16]

Others warn that the use of fingerprints has become common, such as for the use of mobile phones: "The rationale that gave rise to the development of using biometrics in this way is that in 2015 there were 100 million people using mobile phones equipped with a fingerprint reader and this feature was becoming a more widespread offering amongst manufacturers." [17] Reason is simple, as we said, there are no two persons with the same friction ridges, studies have shown that modern automatic fingerprint verification system can successfully distinguish even identical twins. [18] However, safety has a different side - malicious attacker can relatively easily use a false fingerprint.

Finally, what we would like to emphasize is that even other countries out of the EU region also have the similar regulation as the EU.: "Australia has taken an approach similar to the GDPR. Under the Australia Privacy Act 1988, amended in 2014, biometric information are to be used for purposes including verification or identification, and biometric templates are explicitly defined as sensitive personal information." [19]

Given that there is no legal, administrative and judicial practice concerning this problem, finally, we can only give a few basic recommendations. First of all, the most important thing is that fingerprint data is placed in special categories of personal data that are specifically protected. For their use, there should be a voluntary consent of employees - however, employees shouldn't be discriminated if they deny the consent. As for employing the new employees, they should be warned in advance, of the obligation to provide such a consent, but there is no case where we can be sure of the outcome of the dispute, if one of the employees interpret it as a discriminatory measure and ask for protection. In the case where there is an employee's voluntary consent, the data should be kept appropriately – e.g. by the model used by Apple. Any further recording which would allow copying of fingerprint data – certainly isn't allowed. Naturally, companies can avoid the whole problem by using other methods of identification, e.g. by numeric codes, cards and similar. This is also required with the existence of a parallel video surveillance, which is also needed with fingerprint identification, because as we have already written – those are relatively easy to forge. The fact is that fingerprint readers have become widespread, popular and cheap, but on the other hand fingerprints are included in special categories of personal data, which are additionally protected – which has created a number of potential problems in practice, and

we shouldn't forget the penalties for violating the GDPR provisions, which are exceptionally high.

For now, it's impossible to find concrete answers which are required by the practice, because the legal practice will start to create only with the beginning of the application of GDPR. However, it's certainly necessary to further analyse this topic from the legal and technological point of view. In the meantime, we recommend companies to apply technological systems, which will protect employees' biometric data, and by obtaining voluntary consent to use the information, but also a possible application of the other identification systems if the employee's permission cannot be obtained. Certainly, we hope that national regulators will understand the importance of this issue and use the powers of GDPR to resolve this issue by a national regulation, either within the framework of the labour legislation, or within the supplementary regulations on personal data protection.

REFERENCES

[1] Official Journal of the European Union L 119/1

[2] Details of Treaty No.108 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (11 February 2018)

[3] Official Journal L 281, 23/11/1995 P. 0031 – 0050

[4] GDPR FAQs https://www.eugdpr.org/gdpr-faqs.html (11 February 2018)

[5] Hrvatska enciklopedija, entries: Daktiloskopija.

[6] How to Fake Fingerprints https://www.wikihow.com/Fake-Fingerprints (15 February 2018)

[7] About Touch ID advanced security technology, https://support.apple.com/en-us/HT204587 (15 February.2018)

[8] https://www.iso.org/isoiec-27001-information-security.html (17 February 2018)

[9] https://www.techopedia.com/definition/22017/server-room (18 February 2018)

[10] Consolidated Version of the Treaty on the Functioning of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016ME/TXT (17 February 2 2018)

[11] Lj. Mintas Hodak, *Europska unija*, Mate, Zagreb, 2010

[12] P. Carey, *Data Protection*, Oxford University Press, Oxford, 2015

[13] Zakon o tajnosti podataka, Narodne novine 79/07, 86/12.

[14] Processing biometric data? Be careful, under the GDPR, https://iapp.org/news/a/processing-biometric-data-be-careful-under-the-gdpr/ (17 February 2018)

[15] Using biometric data? Sensitive under the GDPR! https://legalict.com/2017/10/18/using-biometric-data-sensitive-under-the-gdpr/ (17 February 2018)

[16] FACTSHEETS / PRIVACY AND MONITORING AT WORK UNDER THE GDPR, https://legalict.com/factsheets/privacy-monitoring-work-gdpr/ (17 February 2018)

[17] Biometric Data and You, https://gdpr.report/news/2017/10/30/gdpr-sensitive-personal-data/ (17 February 2018)

[18] A. K. Jaina, S. Prabhakarb, S.Pankantic, *On the similarity of identical twin fingerprints,* Pattern Recognition, vol. 35, Issue 11, November 2002, p. 2653-2663

[19] Biometric Information as Personal Information—A Brave New World of Regulatory Compliance, https://www.mofo.com/resources/publications/170404-biometric-information-personal.html (15. March 2018)

* Narodne novine is Official Gazette of the Republic of Croatia.