International Journal of Biology and Life Sciences
ISSN: 2957-9511 | Vol. 3, No. 1, 2023

Guardians of Privacy: Understanding the European Union's Framework for Biometric Data Protection

Quan Shi *

School of International Law, China University of Political Science and Law, Beijing, China

Abstract: With the growing prevalence of biometric technology, individual traits are being stored in an increasing number of databases. Users must maintain a high degree of awareness regarding biometric data security. It's important not to provide biometric details without thorough consideration of its necessity, scrutinizing the existing security measures, and understanding the track record of any entity requesting such information. The laws and regulations concerning this matter vary widely depending on the user's location. The European Union is renowned for its stringent personal data protection laws and robust security standards, imposing reporting responsibilities on any entity that collects and requests user data. This article will delve into the regulations and policies surrounding biometric data protection within the European Union.

Keywords: Biometric Data Protection; GDPR; Privacy.

1. Introduction

Biometric data, the unique, permanent, measurable, or collectible biological characteristics used for identity confirmation, is one of the most effective means to identify users. Biometric technology is also highly reliable for users, as unique traits can't be lost or forgotten like combinations of usernames and passwords. Currently, commonly collected biometric features include fingerprints, irises and retinas, voiceprints, facial structures, and DNA profiles. Other biometric traits haven't been widely used yet, but could see more applications in the future, such as body odor, a unique chemical fingerprint that every person carries, or the imprint or structure of the ear, which does not change with age. Biometric data, inherently personal, sensitive, and non-revocable, carries specific risks due to its imperative need for protection. These risks are associated with the storage or comparison of data, the use of biometric authentication systems, and data protection.

The collection and processing of biometric data, given its highly sensitive nature, often entail several stages, including capture, processing, feature extraction, storage, and comparison. All these steps occur within the architectural framework of a biometric system, the design of which has profound implications for data security. An error at any stage could have severe repercussions; for instance, a legitimate user might be wrongly rejected, or an imposter wrongly accepted, leading to potential breaches of security and privacy [1]. The intrinsic vulnerability of biometric systems lies in their probabilistic nature. The data presented for authentication will never perfectly match the reference data stored in the system. This disparity opens a window of opportunity for attackers to exploit the inherent risks, however minimal they might be. Ensuring data security, therefore, requires more than good performance metrics; it calls for a comprehensive strategy that safeguards the data at every stage. This article will discuss the protection of biometric data under the frame of GDPR mechanism.

2. The Concept of Privacy and its Influence Upon EU Data Regulations

Privacy, as a concept, has its roots embedded deeply in some of the most ancient legal principles, serving as the barrier between the public and private spheres [2]. In the 20th century, the right to privacy featured in the 1948 Universal Declaration of Human Rights by the United Nations [3], and subsequently in the 1950 European Convention on Human Rights' Articles 7 ("respect for private and family life") and 8 ("personal data protection") [4]. Moreover, the European Union's Charter of Fundamental Rights, enacted in 2000, which incorporates fifty-four basic human and social rights, binds EU member countries. It holds constitutional value, as confirmed by the 2007 Treaty of Lisbon. However, the notions of "privacy and personal freedom" appeared in European laws and regulations relatively early in the timeline, without a clear definition. For instance, the 1995 Directive referred to "the basic rights and freedoms of natural persons, particularly the right to privacy concerning data processing." This ambiguity in defining fundamental rights was not addressed until the implementation of GDPR, which replaced the broad and unclear term "right to privacy" with the more specific "right to personal data protection." This move established a clear basis of rights for the EU's personal data protection legal system.

In practice, the mechanism for privacy protection in the current EU's General Data Protection Regulation (GDPR) originates from the concept of Privacy by Design, proposed by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, in the late 1990s. As a preventive measure, Privacy by Design emphasizes privacy protection before designing systems that process personal data. It sets forth seven principles, inspired by:proactive and preventive measures in design; default protection (privacy by default); privacy protective measures throughout product design and use; the best and comprehensive protection; end-to-end security – lifecycle protection; visibility and transparency; and finally, respect for user privacy. These seven principles have been widely adopted in the GDPR and have evolved into what is known as "data protection by design

and by default". European data protection laws require data controllers and processors to consider data protection concerns in all aspects of their processing activities. This approach is known as "data protection by design and by default", which is risk-based (i.e., aimed at minimizing risks to individuals) and requires accountability (i.e., organizations must be able to demonstrate how they comply with the law).

3. Biometric Data as Sensitive Data

In May 2018, the General Data Protection Regulation (GDPR) replaced the 95/46/EC Directive issued by the European Parliament and the Council on October 24, 1995, concerning the protection of individuals with regard to the processing of personal data and the free movement of such data. The GDPR defines personal data as any information relating to an identified or identifiable natural person. This includes direct identifiers like name, address, and identification numbers, as well as indirect identifiers like IP addresses and cookie data.

Compared to previous rules, the overarching principle of the GDPR is to enhance the protection of personal data, which is manifested in several specific aspects: Explicit consent is required for data processing; restrictions are imposed on the scope of decisions made in automated processing, such as in personal profiling; specific rights are granted concerning the data collected from particular groups, such as children, including the right to rectification and erasure of data, also known as the right to be forgotten; notifications must be provided in the event of a data breach; more comprehensive and transparent information about data processing must be made available; the right to data portability is allowed, meaning one can transfer their data from one service provider to another; access to personal data is made easier; and stricter assurances are provided when transferring personal data outside of the EU.

Moreover, within personal data, certain information is deemed particularly sensitive. According to the GDPR, the collection or use of these data is prohibited unless the explicit consent of the concerned individual is obtained (active, specific, and preferably written freely given informed consent). These requirements apply to the following data: Data related to personal health; data involving sexual life or sexual orientation; data revealing so-called racial or ethnic origin; political opinions, religious or philosophical beliefs, or trade union membership; genetic and biometric data used for uniquely identifying an individual. Hence, it is undebatable that biometric data falls under the category of sensitive personal information. As such, all biometric identification data should be subject to rigorous protection measures. They should neither be stored in their unprocessed form nor transmitted between two components of a biometric system. Furthermore, this data should not be retained in a format that would allow the reconstruction of any part of the original data.

4. The Specific Rules under GDPR

Article 9 of the GDPR prohibits the processing of biometric data for the unique identification of a natural person, as such personal data is defined as part of a "special category of data" with sensitive nature. However, this prohibition is not absolute; the following key derogations under the same provision of the GDPR can apply in certain limited and restrictive circumstances: The person concerned has given explicit consent; the biometric information is necessary for the controller or data subject to fulfil their obligations in the fields of employment, social security, and social protection law; it is necessary to protect the vital interests of the person who is physically or legally incapable of giving consent; it's necessary for any lawful claims; it is necessary for reasons of public interest in the field of public health. Therefore, many member countries, inspired by Article 9(4) of the GDPR, have formulated their own data protection laws, which provide more restrictions on the handling of sensitive data and limit the situations where exceptions can be applied. For instance, in the Netherlands, according to Article 29 of the Dutch GDPR Implementation Act [5], the processing of biometric data for the purposes of unique identification of a person is allowed, but only within the necessary scope for identity verification or security purposes. This is permitted specifically for the compelling interests related to lawful access to certain places, buildings, services, products, and information systems.

GDPR pays special attention to biometric research in its article 35, introducing the concept of Data Protection Impact Assessment (DPIA). Such an assessment becomes mandatory whenever data processing might lead to a high risk to the rights and freedoms of the individuals involved. The assessment should reveal the nature, the risks, and the mitigations of the processing. All the details can be found in the publications of the European Data Protection Authorities (G29). Therefore, initiating a DPIA becomes necessary when planning to collect biometric identification data. However, it's worth noting that biometric data holds a particular status in the context of public research: The GDPR allows member countries of the EU some leeway, especially in the case of research data. For example, France has chosen to relax some constraints to better align with research objectives. A document named "Overview of the legal regime applicable to processing for the pursuit of scientific research purposes (non-health field)" can be found on the CNIL website, which states: "GDPR broadly defines scientific research. Its recital 159 specifies that processing of personal data for scientific research purposes should be interpreted in a broad manner, covering for example technological development and demonstration, fundamental research, applied research and privately funded research. To reconcile the specificities of research with the necessity of personal data protection, a special framework is provided for these processes." [6]

Indeed, in addition to these specific measures, general rules must also be respected. According to Article 5.1-c) of the GDPR, the principle of relevance and data minimization must be respected. This means that only necessary data should be collected and processed, and excessive or irrelevant data should be avoided. When it comes to the implementation of pseudonymization, the process involves substituting identifiable data fields in a record with pseudonyms or artificial identifiers. This must be executed when it is deemed appropriate. To ensure a data-individual link, the information needed for this link must be stored separately and subject to organizational and technical safeguards. The development of a secure and controlled access system is another critical aspect. It should take into account the data's sensitivity and potential future uses. The primary focus of this system is to restrict data access to only those who are authorized, hence protecting the data. Lastly, performing a data protection impact analysis is almost always a systematic requirement. This essential procedure is a tool that helps identify, assess,

and minimize or mitigate privacy risks associated with data processing activities, reinforcing an organization's commitment to the protection of personal data.

It's crucial to highlight the distinction between pseudonymization and anonymization. Pseudonymization, which is mandated and referred to in Article 32 of the GDPR, entails separating data that can identify an individual from other information. An instance where this approach is specifically advised is in the dissemination of court judgments in public data, as mentioned in the Cadiet report dated October 7, 2016. Technically speaking, encryption is a form of pseudonymization that renders data illegible to anyone without access to the decryption key. This measure substantially enhances the security of data in the event it is compromised. Another method is key-based hashing, which computes a hash while maintaining a level of confidentiality, particularly useful during data transmission [7]. Both encryption and hashing are reversible processes, meaning the original data can be reconstructed. As previously noted in the context of data security, the reversibility of these methods is essential for ensuring that personal data remains accessible when necessary. Anonymization, on the other hand, operates differently. It's an irreversible process. Through a variety of techniques applied to data, attributes, and/or data structures, identification is rendered impossible by the removal or alteration of data. This kind of process results in an anonymized dataset, which doesn't contain any personal data that can be linked back to an individual [8]. Anonymization effectively mitigates GDPR restrictions, as the data no longer contains information pertaining to identifiable individuals. However, anonymization is still subjected to a certain number of limitations, such as the size of the dataset. Therefore, if anonymization techniques are used, an evaluation of the anonymization technique can be made based on point d) of Article 32 of the GDPR. Namely, a good anonymization evaluation scheme is principally based on three criteria: i) is it always possible to isolate an individual (individualization)? ii) Can records related to an individual always be linked (correlation)? iii) Can we infer information about an individual (inference)?

5. Conclusion

Every technology is a double-edged sword. While we consider the convenience brought about by the uniqueness of biometric data, we must not forget the risks it entails. It's critical to strike a balance between the benefits and drawbacks of using biometric data. Biometric systems, despite their potential for improving security and convenience in various aspects of our lives, present significant privacy risks due to the inherent sensitivity of the biometric data they collect and process. Misuse or unauthorized access to this data can result in serious harm, including identity theft and other forms of fraud. Hence, rigorous data protection measures, legal frameworks, and ethical considerations must be in place to ensure the safety and privacy of individuals. Policies like the GDPR provide a blueprint for how to handle biometric data responsibly, but it's the responsibility of the organizations and individuals who use this technology to make sure these rules are strictly followed. Moreover, developing methods like anonymization and pseudonymization further help in maintaining the privacy of the individual's data while still utilizing it for necessary purposes. In the end, the key lies in responsible and ethical use of the technology, with a firm commitment to protecting personal privacy and data security.

References

[1] Pizzi, Gabriele, et al. "Privacy concerns and justice perceptions with the disclosure of biometric versus behavioral data for personalized pricing tell me who you are, I'll tell you how much you pay. Consumers' fairness and privacy perceptions with personalized pricing." Journal of Business Research 148 (2022): 420-432.

[2] Gormley, Ken. "One hundred years of privacy." Wis. L. Rev. (1992): 1335.

[3] Assembly, UN General. "Universal declaration of human rights." UN General Assembly 302.2 (1948): 14-25.

[4] Besson, Samantha. "Enforcing the child's right to know her origins: Contrasting approaches under the convention on the rights of the child and the European convention on human rights." International Journal of Law, Policy and the Family 21.2 (2007): 137-159.

[5] Netherlands - Data Protection Overview: https://www.dataguidance.com/notes/netherlands-data-protection-overview.

[6] CNIL, "biometriques": https://www.cnil.fr/fr/biometrie.

[7] Stalla-Bourdillon, Sophie, and Alison Knight. "Anonymous data v. personal data-false debate: an EU perspective on anonymization, pseudonymization and personal data." Wis. Int'l LJ 34 (2016): 284.

[8] Majeed, Abdul, Safiullah Khan, and Seong Oun Hwang. "Towards Privacy Preservation using Clustering based Anonymization: Recent Advances and Future Research Outlook." IEEE Access (2022).

[9] European Union: General Data Protection Regulation: https://gdpr-info.eu/.