Personal Data under the GDPR: Implications and Challenges

Suraj Karakulath

Constructor (Jacobs) University Bremen

MDSSB-LAW-01 (IT Law)

Dr. Ioannis Revolidis

18.06.2023

Introduction

In today's hyperconnected world, personal data has become a valuable commodity, fueling the digital economy and enabling various online services. However, as more of our lives become reliant on digital services, it becomes critical to ensure that our personal data is protected. The General Data Protection Regulation (GDPR) implemented by the European Union (EU) seeks to accomplish this by establishing comprehensive guidelines for the collection, use, and storage of personal data. This paper aims to shed light on the notion of personal data under the GDPR, exploring its significance and the challenges faced by average users when accessing digital applications.

The importance of personal data protection cannot be overstated. Individuals routinely share their personal information online, both voluntarily and involuntarily, entrusting it to various digital platforms and applications. This information ranges from basic identifiers like names and addresses to more sensitive data such as financial details, health records, and web browsing habits. The ease with which such data can be collected and processed have raised concerns about privacy breaches, unauthorized access, and the potential for misuse or exploitation.

Average users, often unaware of the full extent of data processing practices, face significant challenges in navigating the digital landscape. They encounter complex privacy policies, lengthy terms of service agreements, and hidden data-sharing practices. The lack of transparency and control over personal data can lead to a sense of vulnerability and distrust among users. Furthermore, the proliferation of online services and the sheer volume of data exchanged pose practical challenges in understanding and managing personal data across multiple platforms.

The GDPR addresses these challenges by establishing a comprehensive framework for personal data protection. It introduces key principles such as purpose limitation, data minimization, and accountability, aiming to strike a balance between individual privacy rights and the legitimate interests of data controllers. The regulation grants individuals greater control over their data, empowering them with rights to access, rectify, and delete their personal information.

Despite the GDPR's intentions, the average user faces obstacles when accessing digital applications. Understanding complex privacy policies, exercising data subject rights, and navigating consent mechanisms can be overwhelming for individuals without specialized knowledge or legal expertise. Moreover, technological advancements, such as sophisticated data analytics and the Internet of Things (IoT), present new challenges in assessing the identifiability of personal data and ensuring compliance with the regulation.

This paper delves into the notion of personal data under the GDPR, providing insights into its importance and the challenges encountered by average users. It examines the legal framework, analyzes ambiguities surrounding identification and identifiability, and explores the implications for individuals' daily activities. By shedding light on these issues, this research aims to contribute to a better understanding of personal data protection and foster discussions on the need for user-centric approaches to privacy in the digital age.

Personal Data under the GDPR: Implications, Challenges, and Ethical Considerations

In a world that is becoming increasingly digitalized and data-reliant, the need to protect personal data has become a concern of paramount importance. The European Union (EU) has been leading the way in this regard over the years, recognized the value of a comprehensive legal framework to safeguard individuals' privacy rights. With this in mind, the General Data Protection Regulation (GDPR)[1] was introduced on May 25, 2018, aiming to establish a set of rules across EU member states regarding the processing of personal data.

The GDPR places great importance on defining and protecting personal data, as it recognizes that individuals should have control over their own information. By understanding the notion of personal data under the GDPR, we can explore the potential ambiguities that may arise and assess how this legal framework impacts people's day-to-day activities.

Defining Personal Data under the EU GDPR:

To understand what constitutes personal data under the EU GDPR, the best source to refer would be the precise text in the regulation. Article 4 (1) of the GDPR defines personal data as “any information relating to an identified or identifiable natural person ('data subject')”.

Natural person is a term that GDPR uses to distinguish from “legal persons” such as companies, whose data is not considered personal data[2]. The individual in question must also be

[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), published in Official Journal of the European Union, L 119, 4 May 2016.

[2] What is considered personal data under the EU GDPR? - GDPR.eu. (n.d.). GDPR compliance. Retrieved June 18, 2023, from https://gdpr.eu/eu-gdpr-personal-data/

alive as data related to dead persons are not considered personal data in most cases under the GDPR.

This data can include obvious features like names, addresses, and identification numbers but also extends to less apparent information like IP addresses, location data, and online identifiers. Biometric data such as fingerprints, can also work as identifiers and are included in this definition. The scope of personal data encompasses a wide range of data that can directly or indirectly identify an individual.

Personal data is to be contrasted with "anonymous data", which refers to information that does not relate to an identified or identifiable person. Under the GDPR, processing anonymous data is considered acceptable.

It is important to be precise when it comes to the terms identified and identifiable, as it is necessary for assessing the scope of personal data and to ascertain whether an individual's information can be protected under the scope of the GDPR. The GDPR does indeed distinguish between these related but distinct concepts.

Firsty, identification refers to the situation where the identity of an individual can be established using their personal data by a data controller. The 'controller' again is a term that GDPR describes in Article 4 (7) as referring to the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data. This identification can occur when the data controller possesses explicit information that directly links the data to a specific person. For example, if the data controller has access to a dataset which includes a person's name, contact details, or some form of unique identification number, the identification of that person can be straightforward.

An identifiable natural person is one who can be identified, directly or indirectly, by referring to some kind of identifier such as a name, an identification number, location data, or other factors that are specific to the person.

On the other hand, identifiability refers to a scenario where an individual can be indirectly identified based on some available data. This can happen if and when the data alone may not explicitly reveal the person's identity, but additional information or data processing techniques can be reasonably used to identify them. Identifiability considers the potential ability to single out or distinguish an individual from a larger group.

It is also critical to note that the concept of identifiability can be subjective and dependent on the context, and the GDPR acknowledges this fact. There are several factors that are to be considered to determine whether a person is identifiable according to the law such as:

Context and Accessibility: Identifiability must be assessed in light of all the means reasonably likely to be used to identify the person, including technological advancements. Factors such as the availability of additional data sources, advancements in data analytics, or the likelihood of re-identification should be considered.

Pseudonymization and Encryption: If personal data has undergone measures such as pseudonymization or encryption, which significantly reduce the risk of identification, this may impact the level of identifiability. The effectiveness of such techniques and the possibility of reversal or de-anonymization play a role in determining identifiability.

Reasonable Means: Identifiability is measured by considering whether identification can be reasonably accomplished. This evaluation takes into account the effort, time, and resources that a third party would need to allocate to identify an individual. If identification requires disproportionate effort, the person may be considered non-identifiable.

Potential Linkage: The potential for linking the available data with other information to identify an individual is another relevant factor. If the data, even in its anonymized or aggregated form, can be combined with external data sources to re-identify individuals, identifiability exists. For example, two data sets can contain information about the same data subject and in such cases someone can establish through correlation analysis that two records are assigned to a same group of individuals.

Overall, the determination of identifiability requires a case-by-case analysis, taking into account various contextual and technical factors. It is important to note that even if data is not immediately identifiable, it may still qualify as personal data if the means to achieve identification exist or are reasonably likely to be available.

Illustrative scenario 1: Sharing a photo of a group of people on Instagram

For example, consider the scenario of an individual taking a photo of themself with their friends and posting it on a social media platform like Instagram. This picture can potentially include personal data. In this context, if the picture includes identifiable individuals, such as their faces or other distinctive characteristics, it qualifies as personal data. It need not even be the friends of the individual who took the photo, even strangers in the background of the photo can be considered identifiable if their features are visible. Since the GDPR considers photographs as a form of personal data when they can identify individuals, sharing such pictures may be subject to data protection regulations.

Illustrative scenario 2: Does an IP Address count as personal data

Another type of data that can be considered personal is the IP address. This is so because an IP address can be linked to an identified or identifiable individual. In some cases, an IP address may directly identify a person, especially when it is static or associated with a specific device. Moreover, when the IP address is combined with other data or when the internet service provider has information linking the IP address to an individual, it becomes personally identifiable.

However, it's important to note that the classification of IP addresses as personal data depends on factors such as the legal jurisdiction and the specific context in which the IP address is processed. In certain situations, such as when IP addresses are only used for statistical or analytical purposes without any means of identifying individuals, they may be considered non-personal data.

Ambiguities and Challenges in the Definition of Personal Data

While the GDPR provides a comprehensive definition of personal data, certain ambiguities and challenges persist in its interpretation. One such challenge arises when determining whether certain data can truly identify an individual. The concept of identifiability has led to debates surrounding anonymization and pseudonymization techniques, where the distinction between personal and non-personal data can be blurred.

According to Recital 26 of GDPR, where identification is ‘reasonably likely’ to occur, it constitutes personal data, and where this is not the case the information in question is non-personal. Different national supervisory authorities adopt slightly different interpretation of GDPR in regards to this. For example, the UK Information Commissioner s Office (ICO), stresses that the the risk of re-identification through data linkage is essentially unpredictable[3]. This is because one can never be certain what data is already available or what data may be available in the future. On the other hand, the Irish Data Protection Authority (DPA) states that the data can be considered anonymous if it can be shown that it is unlikely that a data subject will be identified depending on the circumstances of the individual case and the state of technology[4].

[3] Duncan, G., & Elliot, M. (n.d.). Anonymisation: managing data protection risk code of practice. ICO. Retrieved June 18, 2023, from https://ico.org.uk/media/1061/anonymisation-code.pdf

[4] Guidance Note:. (n.d.). Data Protection Commission. Retrieved June 18, 2023, from https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf

Additionally, the advancement of technology poses challenges in determining what types of data fall within the scope of personal information. The proliferation of IoT devices, social media platforms, and big data analytics has created new categories of data that may indirectly identify individuals or enable their profiling. This necessitates ongoing assessment and adaptation of the GDPR to keep pace with emerging technologies.

There is also the issue of the time scale under consideration. Recital 26 requires that the technological developments are also to be taken into account when assessing whether data is personal. But this is not an easy task, as new technological advancements can be rolled out in time which are not yet available to the specific data controller or processor. Take for instance the state of research in quantum computing. It is not obvious whether the potential of this technology in breaking encryption algorithms should be factored in when ascertaining if an encryption technique is capable of transforming personal data into anonymous data[5].

Impact of GDPR on People's Day-to-Day Activities:

The notion of personal data, as defined under the GDPR, has a significant impact on people's daily lives. It makes a significant difference in how individuals interact with technology, service providers, and organizations that process their data. The GDPR helps individuals by granting them certain rights, including the right to access, rectify, and erase their personal data. This heightened awareness and control over personal information have led to increased transparency and accountability in data processing practices.

[5] Quantum computers will break the encryption that protects the internet. (2018, October 20). The Economist. Retrieved June 18, 2023, from https://www.economist.com/science-and-technology/2018/10/20/quantum-computers-will-break-the-encryption-that-protects-the-internet

At the same time, GDPR has had a profound impact on our daily activities, particularly when it comes to working with personal data. These regulations are designed to safeguard individuals' privacy rights and impose certain limitations and responsibilities on how personal data can be processed. We discuss below some of the limitations and considerations one would face when working with personal data.

Consent Requirement:

Using another person's personal data without their consent is generally not permissible under data protection laws. Consent serves as a fundamental principle for lawful processing. To obtain consent, specific conditions must be met:

- Freely Given: Consent must be voluntary and not obtained through coercion or imbalance of power.
- Informed: Individuals must have sufficient information about the processing activities, including the purpose, data categories, and potential third-party disclosures.
- Specific and Unambiguous: Consent should be clear and specific for each processing purpose, leaving no room for confusion.
- Revocable: Individuals should have the right to withdraw consent at any time.

Consent is just one legal basis for processing personal data, but it is often the most applicable in everyday situations involving individuals' data.

Other Legal Grounds:

Beyond consent, there are other legal grounds that may allow the processing of personal data without explicit consent. These include the following scenarios[6]:

- Contractual Necessity: If processing is necessary to fulfill a contract with the individual, their consent may not be required. For example, processing customer data to deliver a purchased product or service.
- Legal Obligations: Processing personal data may be justified if it is required to comply with legal obligations imposed on the data controller. For instance, retaining certain financial information for tax purposes.
- Legitimate Interests: Processing personal data may be permissible if it is based on the legitimate interests pursued by the data controller or a third party. However, this must be balanced against the individuals' rights and freedoms, requiring a legitimate interests assessment.

These alternative legal grounds allow for limited exceptions to the consent requirement but are subject to strict conditions and must be justified based on the specific circumstances of the data processing.

To illustrate the idea of consent more clearly, we revisit a scenario similar to the Instagram photo discussed earlier. Consider the case of a user who comes across a friend's Instagram photo in their feed. In this context, the GDPR places importance on obtaining valid consent from the friend before using or processing such data. Therefore, if the user intends to use their friend's Instagram pictures, it is generally required to seek the author's explicit consent.

[6] González, E. G., & de Hert, P. (2019, February 05). Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. Springer Link. https://link.springer.com/article/10.1007/s12027-018-0546-z

This consent, according to the GDPR should also adhere to specific conditions to ensure it is freely given, informed, specific, and revocable. Firstly, consent must be freely given, meaning it should not be coerced or obtained under any form of undue pressure. It should be a voluntary choice made by the friend. Additionally, consent should be informed, providing the friend with sufficient information regarding the purpose and scope of the data processing, any potential third-party disclosures, and any other relevant details that would enable them to make an informed decision.

Moreover, consent must be specific, meaning it should be obtained separately for each distinct purpose of data processing. This ensures that the friend has clarity about how their data will be used and allows them to exercise control over different aspects of their personal information. Furthermore, valid consent should be revocable at any time, providing the friend with the ability to withdraw their consent if they change their mind or no longer wish to allow the processing of their data.

While consent is typically the primary legal basis for processing personal data, the GDPR does provide some alternative grounds that may allow limited processing without explicit consent. These grounds include contractual necessity, legal obligations, and legitimate interests. For example, if processing the personal data is necessary to fulfill a contract with the individual, consent may not be required. Think for example, a business partnership that the user has with their friend, which allows the user to use the friend’s photos for commercial purposes, that may or may not benefit mutual parties as per the contract. Similarly, certain legal obligations may justify processing personal data without explicit consent, such as retaining financial information for tax purposes. Additionally, processing based on legitimate interests may be permissible if it is balanced against the individuals' rights and freedoms, requiring a legitimate interests assessment.

However, it is important to note that these alternative grounds must be carefully evaluated in each specific scenario, considering the specific context and potential impact on individuals' privacy rights. While they provide limited exceptions to the consent requirement, organizations and individuals should strive to obtain explicit consent whenever feasible, as it represents a transparent and respectful approach to data processing that respects individuals' autonomy and privacy preferences.

When working with personal data, it is essential to respect the principles of data protection, such as purpose limitation, data minimization, and storage limitation. Data controllers must ensure that personal data is processed securely, protected against unauthorized access, and not retained longer than necessary for the stated purpose.

Furthermore, the GDPR has compelled organizations to implement privacy-by-design principles, ensuring that data protection is an integral part of the development of products and services. People now encounter enhanced privacy notices, consent mechanisms, and mechanisms for data portability, giving them greater control over their data.

However, the GDPR's impact is not limited to individuals alone. Organizations and businesses have been required to adapt their data processing practices to comply with the regulation. This has led to changes in data governance, increased security measures, and heightened awareness of privacy-related risks.

Conclusion

The GDPR's definition of personal data forms the cornerstone of privacy protection in the European Union. This term paper has explored the notion of personal data under the European Union's General Data Protection Regulation (GDPR) and its impact on people's day-to-day activities. We have examined the concept of identification and identifiability, the requirements for obtaining valid consent, and the grounds beyond consent that may allow the processing of another person's personal data. We have also reflected on the implications of data protection law on both personal and professional contexts, highlighting the limitations and ethical considerations associated with working with personal data.

Specifically, when using personal data shared on platforms like Instagram, it is essential to recognize that such data falls within the scope of the GDPR. While it may be tempting to use a friend's Instagram pictures without explicit consent, the principles of the GDPR require obtaining valid consent before processing personal data. At the same time, there may be alternative grounds beyond consent that may allow the processing of personal data. It is important however, for organizations and individuals to exercise caution and conduct a careful assessment of the specific context to ensure compliance with the GDPR and respect individuals' privacy rights.

References

Duncan, G., & Elliot, M. (n.d.). *Anonymisation: managing data protection risk code of practice*. ICO. Retrieved June 18, 2023, from https://ico.org.uk/media/1061/anonymisation-code.pdf

González, E. G., & de Hert, P. (2019, February 05). *Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles*. Springer Link. https://link.springer.com/article/10.1007/s12027-018-0546-z

Guidance Note:. (n.d.). Data Protection Commission. Retrieved June 18, 2023, from https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf

Quantum computers will break the encryption that protects the internet. (2018, October 20). The Economist. Retrieved June 18, 2023, from https://www.economist.com/science-and-technology/2018/10/20/quantum-computers-will-break-the-encryption-that-protects-the-internet

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 Dat. (2016, May 4). *Official Journal of the European Union*, L 119.

What is considered personal data under the EU GDPR? - GDPR.eu. (n.d.). GDPR compliance. Retrieved June 18, 2023, from https://gdpr.eu/eu-gdpr-personal-data/