Research on Personal Data Protection of EU General Data Protection Regulation

Hu pengnian¹, Qian Wei²

¹ Department of Public Administration, Nanfang College of Sun Yat-sen University, Guangzhou, Guangdong, 510000, China
² Department of Public Administration, Nanfang College of Sun Yat-sen University, Guangzhou, Guangdong, 510000, China

*Corresponding author’s e-mail: 1492689709@qq.com

Abstract. The EU's General Data Protection Regulation (hereinafter referred to as GDPR), which came into effect on May 25, 2018, is the most concerned personal data protection legal document in the world, and it will inevitably have a profound impact on the construction of personal data protection systems in other countries and regions. It is generally believed that the GDPR is a further implementation and extension of the EU's consistent position to strengthen the protection of personal data as a basic right.

1. Foreword

Introduction

The General Data Protection Regulations ("GDPR") passed by the European Parliament on April 14, 2016, will come into effect on May 25, 2018 in EU member states. The scope of the regulation is extremely broad, and any organization that collects, transmits, retains or processes personal information in all EU member states is subject to the regulation. The GDPR has a total of 99 articles, with a complete structure and strict logic. Among them, the "principle" clause in Chapter II is responsible for the outline and provides the basis for the legal processing of personal data. The relevant spirit runs through the whole text.

Figure 1 General Data Protection Regulation
2. Personal data processing principles

Article 5 of the "Principles" section of the GDPR sets out seven personal data processing principles: legality, fairness and transparency, purpose restrictions, data minimization, accuracy, storage restrictions, integrity and confidentiality, and the principle of consistency of rights and responsibilities. Provisions are provided in the first paragraph and the principle of consistency of rights and responsibilities is provided in the second paragraph.

Compared to the predecessor of the 1995 EU Data Protection Directive (hereinafter referred to as Directive 95), GDPR adds two principles: the principle of transparency and the principle of consistency of rights and responsibilities. The principle of increased transparency reflects the EU's consideration and requirements for the exercise of data subjects' rights and the feasibility of supervision. According to the principle of consistency of rights and responsibilities, data controllers need to prove their compliance with other principles, that is, they must bear the burden of proof.

"Legal, fair and transparent" is the most principled requirement throughout the GDPR data collection, processing and utilization process. Among them, the requirement of legality needs to be comprehensively understood with Article 6.

"Restrictions on purpose" and "data minimization" require that the scope of data collection and processing should be limited to the necessary and minimum scope. On the one hand, it stipulates that it is limited to "specific, clear, and legitimate purposes; on the other hand, even based on the foregoing purposes, there must be sufficiency and relevance requirements to achieve the goal of data minimization." "The principle requires that from the dimension of storage time, after the limited purpose is reached, the data controller must not continue to store identifiable data.

The "restrictions on purpose" and "restrictions on storage" both provide for exceptions, that is, archiving based on public interest, scientific or historical research purposes, and statistical purposes. For this exceptional case, Article 89 of the GDPR provides more specific provisions. On the one hand, allowing member states to stipulate restrictions on the rights of data subjects based on these situations; on the other hand, even based on these exceptions, data controllers also need to take adequate security measures to avoid damage to data subjects, including necessary Technical measures and management measures, such as pseudonymization, and to ensure that data processing is minimized.

"Accuracy" and "integrity" point to quality requirements in data storage and processing. The implementation mechanism of these requirements is reflected in the relevant rights of the data subject stipulated in Chapter III, such as the data subject's right of access, correction, deletion (ie right to be forgotten), right to restrict processing, etc.

"Confidentiality" emphasizes the security protection of data, especially for unauthorized or illegal access and processing. This principle of data security and prevention of leakage has reached consensus in major countries and regions, and often attracts high public attention.

3. Legitimacy basis

The first principle to be observed in data processing is legality. Article 6 of the GDPR provides six types of legality basis, and basically follows the relevant provisions of Directive 95. Specifically include: the consent of the data subject, the performance of the contract, the performance of legal obligations, the protection of important interests, the protection of public interests, and the protection of the controller's priority interests.

In practice, the prevailing privacy policies, user agreements, and mandatory disclosure systems are the embodiment and implementation of the consent principle. It can be considered that user consent is the most important basis for the legality of personal data processing. On the one hand, the principle of consent is mainly reflected in the initial collection of personal data, and the data must be collected

---

1 European Commission, 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, EURPEAN COMMISSION, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046(last visited May. 31, 2018).
with the consent of the user; on the other hand, other rights of the user are actually derived rights of the consent right, and the right to know is the effective exercise of the right to consent. The basis of access, right to correction, right to delete (forgotten right), right to restrict processing, right to object, etc. are actually the concrete manifestation of the right to consent in different links and scenarios of data processing. The legislation, policies and judicial practices of various countries, and the construction and concreteness of a large number of rules, also focus on whether the data processor has truly guaranteed the user's right to know and consent. There are several places in the GDPR that provide specific safeguards for implementing the principle of consent. For example, Article 7 specifically specifies the requirements for consent. Regarding the specific form of consent, there are also important guidelines in the preamble.

Article 12 of Chapter 3 of the “Rights of Data Subjects” of the GDPR focuses on the requirement of transparency to ensure the right of the data subject to know. However, whether or not the principle of consent can bear the heavy burden of supporting the foundation of the entire personal data protection system at the present and future of the rapid development of data processing models has faced many questions and challenges.

The other five legality foundations do not require consent as a prerequisite, but all need to follow strict conditions. Among them, "contract performance" considers the agreement between the user and the data processor, including the necessary preparations for the contract, which is still essentially the consent of the data subject. Several other legitimacy foundations reflect the legislator's search for a balance between multiple conflicts of interest. For example, the two foundations of "fulfilling statutory obligations" and 'protecting the public interest' indicate public interest considerations and statutory exceptions to the protection of personal data, and provide that each member state determines the specific circumstances. For these exceptions, Article 6 also provides strict restrictions to ensure that the principles set out in Article 5 can be effectively implemented.

Article 6, paragraph 4, provides for subsequent processing of data. Subsequent processing refers to processing that is not permitted by the data subject and is not permitted by EU law or Member State legislation. In this case, it is the responsibility of the controller to confirm whether the purpose of this new follow-up process is compatible with the purpose for which the data was originally collected and can therefore be allowed. This requirement is likely to add significant costs to data flow and sharing.

For data controllers and processors, in order to prove that their data processing behavior is based on the last five legal basis without obtaining consent, the wording of the law is very difficult, because most of these situations rely on individual judgment and With strict restrictions, it is safer to obtain user consent.
4. The conditions of "Consent"

Personal consent in GDPR refers to the data subject's consent to the processing of their personal data through a written statement or through a clear affirmative action. The expression of will should be freely given, specific, informed and clear. Silence, default checked dialogs, or inactions do not constitute consent.

Article 7 sets out the conditions for consent. Specifically, the article places a responsibility on the controller to prove that the data subject has agreed to the processing of his or her personal data. The second paragraph provides for other matters (commonly including comprehensive user agreement, etc.) in the written statement of obtaining consent. In this case, "agreement should be presented in a form that is significantly different from other matters, easy to understand and accessible, and in clear and common language." Paragraph 3 provides for the right of the data subject to withdraw consent. Paragraph 4 stipulates that if consent to data processing is a prerequisite for contract signing, and such data processing actually exceeds the scope necessary for the provision of services, it will violate the provisions on "consent should be made freely".

Figure 2 GDPR executive
It is worth noting that the European Union used the concept of "explicit consent" when it proposed the draft GDPR, and did not add the "explicit" limit in the end. However, as stated earlier, "silence, default checked dialog, or inaction" does not constitute consent. Although there is room to determine consent by explaining certain behaviors of users in specific situations, given the overall strict protection tendency of GDPR, it is foreseeable that the interpretation space of "non-explicit" consent will not expand much.

Figure 3 personal data

5. Scope of application
The geographic scope of European privacy laws is expanding through GDPR. Because of this expansion of the scope of application, many organizations located outside the EU and not subject to current European privacy laws will have to apply EU privacy laws with the implementation of the GDPR. The GDPR requires these organizations to respond promptly to GDPR's "compliance" requirements.

First, GDPR applies to organizations with establishments in the EU, as long as these organizations process personal data in the activities of the business in the EU (regardless of whether such processing actually takes place in the EU).

The interpretation of the concept of "location" must be broad and flexible. The requirement is for effective, authentic activities (small activities are sufficient) through sustainable venues. The legal form (such as a branch or subsidiary with legal personality) is not a determining factor. Therefore, having a sole representative in the European Union is sufficient to qualify.

It is not required that personal data processing must be performed by the business organization itself. However, it is required that such processing activities occur in the activities of the business organization (usually having both of the above characteristics, but the conditions described in this sentence must always be met). If the activities of the business organization are inseparable from the activities of the parent company (for example, the existence of the business organization is for the economic benefit of the parent company), the relevant personal data processing behavior should be regulated by GDPR.

Therefore, if the activities of business entities (such as branch offices or liaison agents) are inseparable from the processing of personal data by organizations located outside the EU, GDPR should apply.

Second, if an organization does not have a business establishment in the European Union, it does process personal data of individuals in the European Union and such processing is related to the provision of goods or services to individuals in the European Union, regardless of whether such goods or services are charged, GDPR should also apply.
If a non-EU organization intends to provide goods or services to individuals in the EU, it will be considered to provide goods or services in the EU. Simply being able to access the website or its contact details from within the European Union or using the language commonly used in the country in which the organization is established is not in principle sufficient to be considered as having the above intention. Use the language and / or currency of one or more Member States, referrals from customers in the European Union (for example on a website), use of ads in search engines targeting one or more Member States and / or use of top-level domains (such as .eu or .nl) may result in the goods or services being deemed to be provided in the European Union.

Third, GDPR applies to the processing of personal data of individuals within the EU by non-EU organizations, as long as such processing involves monitoring the actions of those individuals and the processing occurs in the EU.

If, in particular, these individuals are tracked on the Internet in order to make decisions about them or to analyze or predict their personal preferences, behaviors, and attitudes, and processing techniques are used in the process to form portraits, etc., it constitutes Monitor behavior.

It is unclear to what extent monitoring will apply to GDPR. In principle, websites that use so-called "tracking cookies" and monitor used applications are covered by the GDPR (as long as those sites process personal data). The European Court of Justice recently ruled that in some cases, dynamic IP addresses can also be considered personal data. Therefore, owners of websites that store dynamic IP address log data may also be subject to GDPR regulations.

6. Conclusion
The entry into force of the European Union's General Data Protection Regulation (hereinafter referred to as the "Regulations ") has opened the curtain on the reform of personal information protection legislation in various countries. The Regulations have made significant changes to the protection of personal information in many aspects, given individuals more information rights and restricted information transaction rules for information processors and controllers. The most fundamental purpose of these changes is to strengthen the information subject. The right to self-determination of information, thereby safeguarding the sovereignty of information among countries; on the other hand, it is also to meet the needs of the development of the information technology era and the construction of a unified digital market.

References
[1] Wang, H.C. (2019) Practical Evaluation and Enlightenment of the General Data Protection Regulation (GDPR). China's prices: 79–81.
[2] Zhang, J.P. (2019) The evolution of EU personal data rights and its implications. Studies in law and business:182–192.
[3] Wu, Y. (2019) On the Enlightenment of EU Data Protection Law Reform to China. Legal and Economic:99–102
[4] Liu, X.C. (2019) Analysis of the EU General Data Protection Regulation. China Market Regulation News: Page 2.
[5] Li Yuan. Research on personal information protection in the era of big data [D]. Southwest University of political science and law, 2016
[6] Nie Shengkui. Research on legal issues of personal information protection [D]. China University of political science and law, 2009
[7] Hong Hailin. Research on civil law protection of personal information [D]. Southwest University of political science and law, 2007
[8] Zhao Lijun. On the right to be forgotten [D]. Jiangxi University of technology, 2019
[9] Ren Xiaoyu. Research on personal information protection of mobile terminal users in the era of big data [D]. Guangzhou University, 2019
[10] Leonid Titkov, Stefan Poslad, Juan Jim Tan. Applied Artificial Intelligence. 2006 (2-4)