REVIEW ON PRINCIPLE CLAUSES OF THE EU GENERAL DATA PROTECTION REGULATION

Written by ***Zhaoxia Deng***

4th Year Ph.D. Candidate, The University of Hong Kong, Hong Kong

INTRODUCTION

Adopted on 14 April 2016 and becoming enforceable on 25 May 2018, the General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world.[i] Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The GDPR's primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[ii] The GDPR has eleven chapters, among which the second chapter of "Principles" provides a basis for the legal processing of personal data, and its spirits run through the whole text. This paper focuses on some of the principal clauses and makes a comparison with that of the American system to provide some enlightenment for the construction of the relevant system in China.

FUNCTION AND ROLE OF THE GDPR'S PRINCIPAL CLAUSES

The right to privacy is part of the 1950 European Convention on Human Rights, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence." From this basis, the EU has sought to ensure the protection of this right through legislation. As its core, GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for businesses in the EU can fully benefit from the digital economy. The reforms are designed to reflect the world we're living in now and bring laws and obligations - including those around personal data, privacy, and consent - across Europe up to speed for the internet-connected age.

Generally speaking, GDPR is the extension of the EU's position to strengthen the protection of personal data as a basic right. This can be reflected in the adoption of the "regulation", a legal document that directly takes effect within the scope of Member States. The GDPR is updated from the 1995 EU Data Protection Directive (hereinafter referred to as "1995 Directive"). The 1995 Directive established the minimum data privacy and security standards, upon which each member state based its own implementing law. However, because of the prerequisite of transforming domestic laws for being taken effect in the Member States, there were still inevitable inconsistencies in legislation and enforcement among countries. In fact, "directives" have long been the main form of coordinating legislation among the EU Member States, while "regulations" are only used to apply to very limited areas, such as competition law and EU trademarks. Therefore, the application of "regulation" is considered "radical" by European scholars.[iii] Of course, this also indicates that the EU is ready to embrace changes in the development and characteristics of the Internet and big data, and fully realizes that the regional nature of legal documents can no longer cope with the flow and processing of data without borders. Although the regulations themselves can be the direct basis for law enforcement in various countries, the localized implementation of the regulations still needs a series of complex supporting systems and institutions due to their different legal systems. It will be a valuable means of coordination for countries to provide a set of basic guiding principles and set their own rules and exceptions according to domestic public policies except for the specific provisions of the unified law enforcement agencies, coordination system, legal responsibility and penalty, and other implementation mechanisms.

In addition to providing guidance and coordination direction for the Member States, another important function of the principal clauses is to lay the basic framework and foundation for the whole text of the regulation. On the one hand, the spirit of the basic principal framework established by the principle clauses runs through the whole regulation, including the rights of the data subject in Chapter III, the obligations of the controller and processor in Chapter IV, and the transfers of personal data to third countries or international organizations in Chapter V, which are the concretization of the principle system. On the other hand, the principal clauses can also be used as the legal basis of direct application, and become the direct measurement standard of the behavior of the data controller and processor to judge whether it has the legitimacy basis. In particular, the data subject's "consent" principle and its specific rules have

become the most important rules to guide the process of obtaining user's consent in practice. The exception to the principle of consent also reflects the EU legislators' consideration of social interests beyond personal data as a basic right and leaves some room for public policy consideration of various countries. Regardless of its actual effect, it also reflects the concept of interest balance and coordination from the legislative perspective.

As for the international influence, the principal clauses follow a series of basic principles shaped in the 1995 Directive and even earlier legal documents, such as purpose limitation, data minimization, accuracy, integrity, confidentiality, etc., which has had an indelible and far-reaching impact on many countries and regions including China for a long time and has profoundly affected and shaped people's awareness of personal data protection. The basic concept has gradually become the consensus of the government, industry, and the public. The principal clauses of GDPR reconfirm and declare these important principles, and continues the important contribution of EU legislative tradition to the establishment and coordination of international rules.

STRUCTURE AND CONTENT OF THE PRINCIPAL CLAUSES

The second chapter of GDPR consists of seven articles from Article 5 to Article 11, which make detailed provisions on the principles, legal basis, special circumstances, and some exceptions of data processing behavior. Among them, articles 5 to 7 are the most direct embodiment of the principal system.

(1) Article 5: Principles Relating to Processing of Personal Data

Article 5 stipulates seven principles for processing of personal data: (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality;(7) accountability. Compared with the 1995 Directive, GDPR adds two principles: the principle of transparency and the principle of accountability. The principle of transparency reflects the EU authorities' consideration and requirements on the feasibility of exercising rights by data subjects and supervision on that data, while under the principle of accountability, data controllers need to prove their compliance with other principles, that is, they need to bear the corresponding burden of proof. As explained in section 85 of the preamble of the GDPR, "As soon as the controller becomes

aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller can demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"[iv].

As the most basic principle, "lawfulness, fairness, and transparency" runs through the whole process of data collection, processing, and utilization. Among them, the requirement of "lawfulness" needs to be understood as a whole with Article 6. The requirements of "purpose limitation" and "data minimization" aim at data collection and processing process, which should be strictly limited to the necessary and minimum scope. That is, it should, on the one hand, be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes",[v] and on the other hand, be "adequate, relevant and limited to what is necessary concerning the purposes for which they are processed".[vi] The principle of "storage limitation" is from the dimension of storage time, requiring that the data controller shall no longer store the identifiable data than is necessary for the purposes for which the personal data is processed.

There are exceptions in terms of the principle of "purpose limitation" and "storage limitation", that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes"[vii]. Article 89 of the GDPR provides more specific explanations for these exceptions. For one thing, member states are allowed to stipulate restrictions on the relevant rights of data subjects based on these circumstances. For another, data controllers should take appropriate technical and organizational measures to avoid damages to data subjects, including pseudonymization, and to ensure respect for the principle of data minimization.

"Accuracy" and "integrity" refer to the quality requirements in the process of data storage and processing. The realization mechanism of these requirements is embodied in the relevant rights of the data subject stipulated in Chapter 3, such as the right of access (Article 15), the right to rectification (Article 16), the right to erasure, or the right to be forgotten (Article 17), the right to restriction of processing (Article 18), the right to object (Article 21), etc.

"Confidentiality" emphasizes the security measures for data, especially for unauthorized or illegal access and processing. This principle for data security and prevention of leakage has

been widely accepted in major countries and regions and often caused high public concern through some public opinion events. For example, in March 2018, the outbreak and continuous fermentation of Facebook data leakage incident made data security and protection become the focus of global Internet regulation once again. This is also one of the most important obligations of "data processor" in Chapter 4 of GDPR[viii].

(2) Article 6: Lawfulness of Processing

The primary principle of data processing behavior is lawfulness. Article 6 of GDPR stipulates six situations of legitimacy basis, which basically copies the relevant provisions of the 1995 Directive. These six situations include the consent of the data subject, the performance of the contract, the compliance with legal obligations, the protection of vital interests, the purposes of public interests and the priority interests of the controller. In practice, the privacy policy, the user agreement and the compulsory disclosure system are the embodiment and implementation of the principle of consent. It can be said that user consent is the most important basis for the legitimacy of personal data processing. Above all, the principle of consent is mainly reflected in the initial collection of personal data, which can only be processed with the consent of the data subject. Furthermore, other rights of users are actually derivative rights of consent right. The right to know is the basis for the effective exercise of consent right. The right to access, the right to rectification, the right to erasure (Right to be forgotten), the right to restriction of processing, the right to object and so on are actually the concrete embodiment of consent right in different links and scenarios of data processing.

The legislation, policy and judicial practice of various countries, as well as the construction and concretization of a large number of rules, also focus on whether the data processor protects the user's right to know and consent. There are also many specific safeguard measures for the implementation of the principle of consent in GDPR. For example, Article 7 specifically stipulates the elements of consent. As for the specific form of consent, there are also important guidelines in section 32 of the preamble. And Article 12 stipulates the requirements of transparency to ensure the right to know of data subjects. However, with the rapid development of data processing mode, whether the principle of consent can still bear the important task of supporting the whole personal data protection system has been a question, which will be discussed separately in the third part below.

The other five situations of legitimacy basis are not on the prerequisite of consent, but they all need to follow strict conditions. Among them, “contract performance” considers the agreement between the user and the data processor, including the necessary preparation for the contract, which is still the consent of the data subject in essence. The other legitimacy bases embody the legislators' concept of balance between various conflicts of interest. For example, “compliance with legal obligations” and “public interest” can be determined by the member states. Section 2 and section 3 of this article also stipulate strict conditions to ensure the realization of the principles of fairness and transparency, purpose limitation, storage limitation, etc. However, there are no specific explanations or practical examples regarding “legal obligations”. It can be speculated that the mandatory obligations of data controllers for public safety and health should be included. While it is still unclear whether the relevant responsibilities based on the tort law and other privacy laws should be the excuses to reduce the right of data subjects, such as collecting user data to fulfil the obligation of “notice-delete”, or scanning the content uploaded by users to fulfil the obligation of copyright technology filtering. In the case of “protecting the vital interests” and “priority interests of the controller”, it reflects the conflict and balance between personal data protection and other interests of the data subject, the interests of the third-party and the interests of the data controller. Whether other interests are “vital” or “overriding” is likely to be judged on a case-by-case basis.

Section 4 of Article 6 stipulates the subsequent processing of data. Subsequent processing refers to processing the personal data for a purpose not based on the data subject's consent or a Union or Member State law. In this case, the controller has the responsibility to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected. This provision may impose a very heavy cost on data flow and sharing. For data controllers and processors, it is very difficult to prove that their data processing behavior is based on the latter five legal bases that they do not need to obtain consent because most of the cases require case judgment and have strict restrictions. Therefore, it is safer to obtain the consent of users. As for the relationship between Article 5 and Article 6, GDPR has not been clearly stated. Therefore, for any legal processing of personal data, we need to meet the basic principles and specific legitimacy requirements.

(3) Article 7: Conditions for Consent

"Consent" of the data subject in GDPR refers to any freely given, specific, informed, and unambiguous indication of the data subjects wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[ix] Section 32 of the preamble provides important guidance on how to determine the "clear affirmative act". Accordingly, "Consent should be given by a clear affirmative action such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services, or another statement or conduct which indicates in this context the data subject's acceptance of the proposed processing of his or her data. Silence, pre-ticked boxes, or inactivity should not, therefore, constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided".[x]

Article 7 sets out the conditions for consent. Especially, it requires that the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.[xi] In case when the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.[xii] It is worth noting that the GDPR did not add "explicit" before "consent" despite that the European Commission used the concept of "explicit consent" when making the draft. However, given the strict protection tendency of GDPR, the interpretation space of "non-explicit" consent will not expand too much.[xiii]

(4) Article 8: Conditions Applicable to Child's Consent in Relation to Information Society Services

The protection of children's information has always been the focus of personal data protection all over the world, and GDPR provides some special provisions on this issue. Article 8 stipulates that "the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental

responsibility for the child".[xiv] The Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.[xv] Besides, Section 2 of this Article requires that "controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility for the child, taking into consideration available technology".[xvi] Yet, despite that the protection of children's rights and interests in cyberspace has long been a highly consensus issue, its real implementation is facing many difficulties, including identity verification, content isolation and data processing, etc. Except for waiting for advanced technology, the protection of children's rights and interests is an area that needs the joint participation and efforts of multiple subjects.

(5) Article 9 & 10: Processing of Special Categories of Personal Data and Data Relating to Criminal Convictions and Offences

The special categories of personal data specified in Article 9 include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation,"[xvii] which is in line with the 1995 Directive. Among them, "genetic data", "biometric data" and "data concerning a natural person's sexual orientation" are newly added in GDPR, reflecting the response to new scientific and technological development and social phenomena.

Article 9 takes the position of a general prohibition on the processing of sensitive data, but at the same time, it provides ten exceptions in section 2. In the first case, the "explicit consent" of the data subject is stipulated, but the member states can also stipulate that it may not be lifted by the data subject; similarly, if the sensitive data is obviously disclosed by the data subject, it can also be processed. Additionally, section 2 also provides exceptions for the data subject in the field of employment, social security, social protection law, and for protecting other vital interests. Although there are many exceptions, each of them has strict restrictions. On the whole, except for the explicit consent or disclosure of the data subject, the space for exceptions is very limited.

Personal data relating to criminal convictions and offenses is also stipulated as a special type in Article 10. This kind of personal information involves the protection of basic human rights in criminal procedure. Therefore, GDPR also imposes strict restrictions on its processing, which must be carried out under the control of official authority or authorized by Union or

Member State law.

(6) Article 11: Processing Which does not Require Identification

GDPR does not require the controller of the data subject who does not need to be identified in the data processing to undertake various responsibilities related to personal data protection. Special controllers do not need to pay extra efforts to protect the rights of the data subject, such as the right of access, right of rectification and erasure, right to restriction of processing, and so on.[xviii] However, if the data subject, to exercise his or her rights under those articles, provides additional information enabling his or her identification, the controller may still have to bear the above obligations.

BOUNDARY OF "CONSENT" PRINCIPLE AND ITS ENLIGHTENMENT TO CHINA

The GDPR contains 99 articles, with a huge structure, detailed content, and rigorous logic. It is based on the basic framework outlined by its basic principles. Hence it is relatively clear and simple in value orientation and protection mode. That is to protect the basic rights of the data subject, which is put forward at the beginning of section 1 of the preamble. Therefore, it is not exaggerated to define GDPR as a basic right protection law. On this prerequisite, it uses the "consent of data subject" as the primary legitimacy basis and to construct the whole system with the core of users' knowledge, consent, choice, and control. As mentioned above, although there are six bases of lawfulness in the principal clause, all the cases other than the "consent" principle are attached with harsh conditions and have a high degree of uncertainty. No matter in theory or practice, at least in the visible future, other cases are difficult to shake the mainstream and basic status of the "consent" principle.

User consent as the dominant principle is the natural result of GDPR as a right protection law. The confirmation of personal control over their data, together with the principle of informed consent, constitutes a typical model of private rights protection. In the era of big data with personal data as the basic resource, the external presentation of personal personality is inseparable from their own data processing, including the provision of goods and services, and the participation in economic, cultural, political, and social life. In this situation, the necessity of giving individuals control over their data to fight against powerful business organizations

and political forces has indeed reached the consensus of most people.

However, the query and reflection on the principle of user consent have never stopped. Although data controllers are required by law to formulate more perfect privacy policies and fulfil more complex notification obligations, this regulatory idea of compulsory disclosure of traditional consumer contracts has always faced the challenge of invalidation. There are also many controversies on the limitations of the principle of informed consent in the field of personal data protection.[xix] Empirical research shows that users rarely read the privacy policy, even when regulators try to simplify the privacy policy text to make it easy to understand. In the face of a lengthy privacy policy, it will bring huge cost when users are required to read one by one. Even if users read the privacy policy, they may not be able to rationally predict the risks they may face. In this sense, it will be the most rational choice to ignore the privacy policy. Hence the "consent" based on the principle of consent is far less meaningful than the legislators expected. The scientificity and effectiveness of the whole data protection and governance framework based on the principle of "consent" naturally deserves a big question mark. Whether it is the EU GDPR whose core is to protect the basic rights of individuals or the FTC law whose core is to protect the interests of consumers and privacy expectations in the United States, their common foothold is to protect the interests of users. Therefore, whether the subjective wishes of users are respected has become the most important consideration. Although the EU and the US have adopted different paths and given different weights to legal intervention and market regulation, they have the same basic starting point. Therefore, the user agreement is always the core issue of common concern of the two modes.[xx]

Yet, even if user consent is a mechanism without the concern of losing effectiveness, it may not be complete to achieve the policy goal of personal data protection. Data protection may have other dimensions of policy objectives, such as security, risk prevention, industrial policy, etc. GDPR takes into account the demands of security and public interest through the provision of exceptions, with the form of limiting the rights of the data subject. However, data protection is not always in conflict with security and public interest, especially in terms of national and sovereign interests. National security and public interest may become the legitimate basis for data protection. At this level, the relevant principles and rules of personal data protection are introduced into the field of "network security law" in our country. In addition to the protection of individual rights, it, more importantly, reflects the concern of legislators for the security

interests beyond the individual. The personal data protection system based on security, risk prevention, and other value goals can not only consider the protection of private rights but also need to go beyond the "consent" mode and establish a supporting system in line with specific value goals.[xxi]

The more stringent user consent requirements can also restrict and hinder the data flow and sharing. The rise and rapid development of the Internet and data industry are largely based on the free flow of data as the basic resource. "Interconnection" and the innovation and change of technology and business model require the open utilization and integration of big data. GDPR strictly limits the possibility of data subsequent processing, which has caused a lot of "inappropriate" queries. Especially in the era of IOT and the rise and vigorous development of AI, GDPR adheres to the traditional (or even ancient) rights protection mode, which is likely to cause serious obstacles to the development of the industry.[xxii] In this sense, in the process of building China's personal data protection system, it is reasonable to systematically reflect on GDPR's a bit strict and mechanical consent principle and its supporting system, as well as considering China's main demands and value orientation, to actively carry out the system innovation and uphold a more open and friendly attitude towards industrial development. The dynamics and flexibility of rules which are designed through the bottom-up and distributed rule generation mechanism will shape more in line with the needs of China's personal data protection system.[xxiii]

ENDNOTES

[i] The EU General Data Protection Regulation (GDPR) 2016/679.
[ii] Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)' Interinstitutional File 2012/0011(COD), Brussels, 11 June 2015. <https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf > last visited December 12, 2020.
[iii] Rong Wang, 'Detailed Explanation of EU General Regulations on Data Protection' (2016) Issue 4 Dig Data.
[iv] Section 85 of the Preamble of the GDPR.
[v] Article 5 section 1(b) of GDPR.
[vi] Article 5 section 1 (c)of GDPR.
[vii] Article 5 section 1 (b) & (e) of GDPR.
[viii] See Article 32-34 of the GDPR.
[ix] Section 11 of the Preamble of GDPR.
[x] Section 32 of the Preamble of GDPR.
[xi] Article 7 (1) of the GDPR.
[xii] Article 7(2) of the GDPR.
[xiii] Paul De Hert & Vakiris papakonstandino, 'New General Data Protection Regulation: Is It Still A Perfect System to Protect Individuals?' 2018-1-28, http://www.dgcs-research.net/a/xueshuguandian/2017/1230/4.html last visited December 22, 2020.

[xiv] Article 8(1) of the GDPR.
[xv] Ibid.
[xvi] Article 8(2) of the GDPR.
[xvii] Article 9 of the GDPR.
[xviii] See Article 15 to 20 of the GDPR.
[xix] Rong Wang, 'Detailed Explanation of EU General Regulations on Data Protection' (2016) Issue 4 Dig Data.
[xx] Daniel Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 26 Harvard Law Review 1880.
[xxi] Wei Fan, 'Reconstruction of Personal Data Protection System in the Era of Big Data' (2016) Issue 5 Global Law Review.

[xxii] Paul De Hert & Vakiris papakonstandino, 'New General Data Protection Regulation: Is It Still A Perfect System to Protect Individuals?' 2018-1-28, http://www.dgcs-research.net/a/xueshuguandian/2017/1230/4.html last visited December 22, 2020.

[xxiii] Xiaochun Liu, 'Industrial Standard Leading Mode of Personal Data Protection in the Era of Big Data' (2017) Issue 2 Law and Economy.