The Application of Transparency of Personal Data Processing in GDPR
——The WhatsApp Case as an Example

Henghao Li[1,a]

[1] *ISTITUTO ITALO-CINESE*
[a]*Email: lhh0403@foxmail.com*

ABSTRACT
The issue of transparency in data processing is becoming more important with the development of information society. The WhatsApp case, as the case with the largest amount of transparency fines until now, is quite representative. In this case, the commission's case handling procedures, requirements of data processing notification methods and content are of practical significance. Therefore, Chinese legislators can improve the flexibility of data identification and scenario-based legislation, and enterprises need to improve their services of notification obligations and data subject's rights.

Keywords: *personal data, transparency, data compliance, GDPR*

1. INTRODUCTION

With the development of new technologies such as artificial intelligence and big data, personal data has become more important in modern industries and even regarded as a resource like oil [1]. At the same time, due to the continuous popularization of information infrastructure, the post-information society will be built on network interconnection and social intelligence [2]. Therefore, large-scale data processing is inevitable, and the problem of transparency of data processing will follow. For this reason, a lot of legislators of different countries approved the transparency content in the data protection legislation. For example, the Article 7 of the Personal Information Protection Law of China stipulates that the handling of personal information should follow the principles of transparency, and Article 5 of the EU General Data Protection Regulation stipulates the principle of transparency in processing personal data. These laws show the importance of transparency in data processing.

In September 2021, the Irish Data Protection Commission announced its decision of the WhatsApp case, which imposed a fine of 225 million euros for violations of transparency of GDPR, which became the largest case of transparency fines in GDPR until now. The case lasted for about three years and analysed various aspects in processing of personal data in GDPR. Therefore, this article will analyse the case and try to make suggestions on Chinese legislation and the activities of Chinese companies.

2. THE SITUATION OF THE CASE

After receiving complaints about WhatsApp's illegal handling of personal data transparency, the Irish Data Protection Commission began to investigate in December 2018. The investigation mainly related to WhatsApp's compliance with GDPR's transparency obligations and issued The Draft Report [3] in September 2019. The report made conclusions on WhatsApp's violation of Articles 12, 13, and 14 of GDPR.

In December 2020, the commission issued The Composite Draft [3] which based on the report and submitted it to supervision agencies. The SA of eight states (including Germany, Poland, and France) opposed and exchanged comments in January 2021. The EDPB finally issued a decision in July 2021, and the Irish Data Protection Commission made the decision in September 2021:

WhatsApp violated Article 5(1)(a), Article 12, Article 13, and Article 14 of GDPR, with fines of 90 million, 30 million, 30 million, and 75 million, for a total of 225 million euros. [3]

3. CASE ANALYSIS

3.1. The procedure for handling transparency cases of GDPR

According to the analysis, the European Court of Justice generally separates the processing of personal data into two parts: "personal data" and "personal data processing" when it protects personal data [4]. In this case, the Irish Data Protection Commission's decision on the transparency of personal data processing is mainly divided into five parts: (1) transparency in the context of non-users (the main analysis content is whether non-user data can be recognized as personal data), (2) transparency in the context of users, (3) transparency in the context of sharing of user personal data, (4) extent of compliance with the principle of transparency, (5) exercise of corrective powers. [3] (Figure1) It shows the decision of this case has similarities with the judgment of the European Court of Justice. As a representative case, the summary of the procedure for handling this case can also provide a reference for subsequent research on other transparency cases in GDPR.

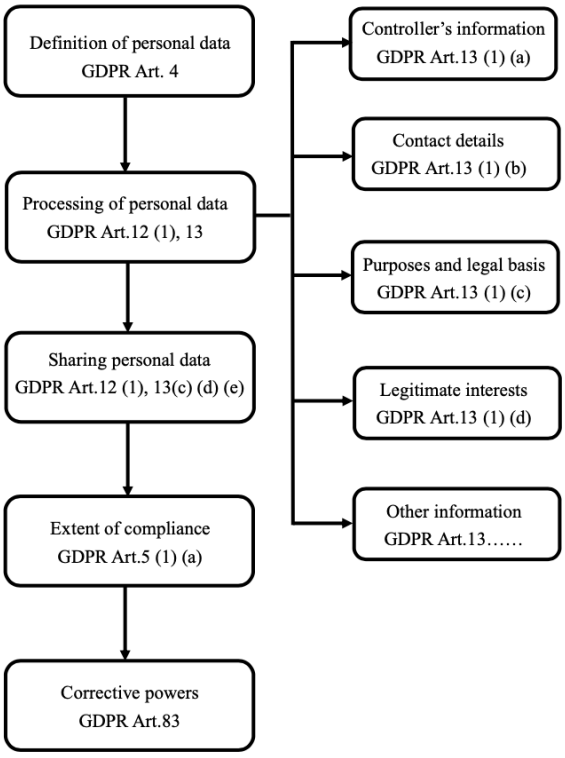

Figure 1 The procedure

3.2. The notification method of data processing with transparency requirements

According to Article 12(1) of the GDPR, information should be provided in a concise, transparent, intelligible and easily accessible form. Conciseness means that the content of the information is simple and clear. Transparent means that the information given to users from the data controller should be unconcealed and complete. Intelligible means that the content of the information received by the data subject should be written in a way that ordinary people can understand. Easily accessible means that the type of information is easily available to the data subject, without too many steps.

Regarding this standard of information notification, WhatsApp is considered as insufficient. At first, the information it provides is not complete and enough sections that are easy for users to read, so it does not meet the requirements of concise and intelligible. Secondly, when WhatsApp provides information, it attaches large number of links to connect to the additional text [3], which also complicates the reading of the information to some extent, so it does not meet the requirements of easily accessible.

3.3. The notification content of data processing with transparency requirements

According to Article 13(1)(c) of the GDPR, the data controller shall clearly inform the purpose and the legal basis of data processing. The purpose needs to be specific, clear, and valid. The legal basis refers to the lawful conditions based on Article 6 of GDPR. According to Article 6(1)(a), one of the sources of lawfulness of processing is the consent of the data subject. The consent needs to be established on the premise that the data subject has fully understood the purpose for which the data is processed. However, due to complex legal terminology and other reasons, it is becoming more and more difficult to agree in practice [5]. If the data subject does not fully understand the purpose, the consent given by the data subject may be a consent with insufficient information, and the lawfulness of the data processing will be questioned.

Therefore, to ensure the lawfulness of the data subject's consent, the data controller should clearly inform the purpose of the whole information processing. In this case, although WhatsApp stated the purpose of information processing in the "Information We Collect" [3] part of the privacy policy, the investigation showed that it only pointed out the purpose of the information was to provide services and did not clearly describe what specific way it would use. Therefore, the data subject may not know the specific purpose and operation method of WhatsApp when it processes the data. Finally, WhatsApp violate Article 13(1)(c) of the GDPR.

4. SUGGESTIONS ON TRANSPARENCY OF PERSONAL DATA PROCESSING

4.1. Legislators

4.1.1. Strengthen the flexibility of personal data identification

With the advancement of technology, the identification of personal data is constantly changing. Originally, through de-identification, personal data can be successfully anonymous. Now it is possible to re-identify the data subject through the combination of certain algorithms and the environment. In this case, WhatsApp used lossy hash to anonymize personal data, but in the end, there is still the possibility of identifying the data subject through other ways. [3]

Therefore, the identification of personal data should be more flexible. For example, the legislator can establish a "reasonably possible" determination standard. It is not only considering factors such as technology, but also allowing data controllers or third parties to list all possible ways [6], which means that it will be more flexible in confirming personal data. At the same time, legislator can also consider adopting a tiered and classified legislative approach to determine different levels of personal data. Establishing different identification standards of different data can prevent the high cost of adopting the same identification requirements for both important and unimportant data.

4.1.2. Scenario-based legislation on personal data transparency

Information is dynamic and diffuse, which will transform into each other in specific application scenarios. [7] Therefore, to analyse personal data in different scenarios, GDPR established multiple layers of transparency [8]. It can also be found in WhatsApp case. When determining the transparency of the use of personal data, the Irish Data Protection Commission adopted a method of identifying them in different scenarios (such as data transmission and storage [3]).

Therefore, Chinese legislation can adopt the method and make requirements for transparency with different data usage scenarios. For example, classifying transparency by the whole process of data processing. Dividing it into data collection, recording, storage, modification, use, transmission and other scenarios, and setting different transparency standards with different characteristics of various scenarios. It is also possible for distinction with different rights of the data subject. Dividing them into scenarios such as the right to know, the right to access, the right to delete, the right to portability, etc., and the detail of requirements of transparency will rely on different rights. With the clear scenario-based legislation, the predictability of the law can be ensured, and judicial practice will also have a clearer direction. Judges can have clearer judgment standards, and enterprises can have a clearer data compliance basis.

4.2. Enterprise

4.2.1. Improve the transparency requirements of information disclosure obligations

It can be found that the data subject may face the issue of enterprise's notification obligation during personal data processing. Through inadequate notification obligations and cooperating with algorithmic black-box operations, enterprises can gain benefits and infringe citizens' personal data rights. Therefore, the Personal Information Protection Law of China, GDPR, the California Consumer Privacy Act of the US all stipulate the principle of transparency. So there should be a judge between the benefits and punishment of violating notification obligations of transparency, or a balance between transparency and benefits will not be achieved. [9]

When processing personal data, enterprises should first clearly inform the purpose of processing, legal basis, contact information and content with local legal requirements, so that consumers can understand the data policy and agree to these behaviours [10]. Secondly, the disclosure of information should also meet the requirements of concise, transparent, intelligible and easily accessible. It should be putted together as much as possible and described in simple language to prevent a punishment like Google, whose information was considered as "general and vague". Only by meeting the requirements above can it be ensured that data subjects' rights are protected when data is being used. At the same time, the punishments for illegal information disclosure can also be avoided.

4.2.2. Meet the transparency requirements of the data subject's rights

When an enterprise enters a market of a scope of law, it should provide services in accordance with the rights of data subjects of local law to make sure the enterprise's data compliance. For example, GDPR stipulates multiple rights such as the right to be informed, the right of access, the right to rectification. The Personal Information Protection Law of China stipulates many rights like the right to be informed and the right to portability. Obligations such as GDPR are set to force enterprises to take data protection into consideration seriously [11]. In this case, after WhatsApp promised to give users the right to withdraw consent, it did not mention how to use the right, which in fact, created obstacles for data subjects.

In the short term, the lack of satisfaction of the

transparency obligations of data subjects' rights seems to make enterprises less responsibilities, and costs are also reduced. However, in the long run, if data subjects find that their data rights are restricted or concealed, and do not understand the purpose of processing of their data, they will choose to give up the enterprise's services. In addition, failure to comply with local transparency requirements may result in punishment of local supervisory agencies, which increases the compliance cost of the company. Therefore, enterprises should ensure the transparency requirements when providing rights. So that data subjects can exercise all the data rights.

5. CONCLUSION

With the continuous progress of the information society, the importance of personal data has become increasingly prominent. This article analyses the WhatsApp case to understand the EU supervisory agencies' decision logic, the method and content of notification in transparency-related cases of GDPR. In addition, putting forward suggestions about transparency on Chinese legislation and Chinese enterprises. However, it is not enough to analyse the transparency of personal data processing in just one case. It is necessary to learn more about EU legislation and cases to promote the standardization of personal data transparency both in legislation and practice in the future.

REFERENCES

[1] Duncan E. Osborne, Truth, Transparency, and the Right of Privacy, ACTEC Law Journal, 2021.

[2] Feng Wang, Privacy or Transparency: The Privacy Dilemma in Smart Society and Its Governance, Administrative Tribune, 2021, pp. 98-104.

[3] Data Protection Commission, In the matter of the General Data Protection Regulation—— DPC Inquiry Reference: IN-18-12-2, 2021.

[4] Peiru Cai, Research on the Right to the Protection of Personal Data in EU，The Jurist, 2021, pp. 16-30, 191-192.

[5] Damian Clifford, Inge Graef, Peggy Valcke, Pre-formulated Declaration of Data Subject Consent-citizen-consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections, German Law Journal, 2019.

[6] Jie Jiang, Zhou Lan, Yiran Qi, The Type Deconstruction of Personal Information De-recognization and Related Governance Mechanism, Library & Information, 2021, pp. 79-86.

[7] Qihua Sun, The Reconfirmation of the Legal Interest of the Crime of Infringing on Citizens' Personal Information—— Taking the Contextual Integrity Theory as the Analytical Framework, Western Law Review, 2021, pp. 80-90.

[8] Margot E. Kaminski, The Right to Explanation, Explained, Berkeley Technology Law Journal, 2019, pp. 190-217.

[9] Tal Z. Zarsky, Transparent Predictions , University of Illinois Law Review, 2013.

[10] Matt Sneed, The Key to the Regulating Facebook and Data Collection Companies is Transparency, Albany Law Journal of Science and Technology, 2020.

[11] Meg Leta Jones, Margot E. Kaminski, An American's Guide to the GDPR, Denver Law Review, 2020, pp. 94-127.