The General Data Protection Regulation And The Implication On Cross-Border Business

Pavitpok Kittima

Abstract

In the digital age, the growth of information and the complexity of borderless cyberspace have raised critical issues on both business model and jurisdiction. The unilaterally extraterritorial legislation of the General Data Protection Regulation (GDPR) adopted by the European Union in 2016 mainly aims to harmonize the data privacy law and push the EU to a digital single market. For international businesses which are the trade partners of the EU, while the Regulation reduces the burdens through a single-set law across the EU and potentially enhances market opportunity and competitive growth, the extraterritorial effects of the Regulation also pose a new challenge to international trade mechanism, particularly in term of the business model, the administrative costs. Therefore, the understanding of mechanisms regulated in the Regulation including its opportunity and concern will help the international companies for establishment their internal governance schemes in compliance with the EU data protection law.

Keywords: GDPR, the Regulation, cross-border business

1. Introduction

The dramatic growth of Internet network and widespread of information infrastructure are factors to impact on international production and trade pattern. Digital technologies are critical to Europe’s economic growth with growing seven times the rate of the rest of the economy. Cyberspace is identified as a global common. It is characterized by anonymity and ubiquity, its space or place is difficult to link with the geographical boundaries. With the distinctive characteristic of borderless, it has raised critical issues with far-reaching implication, such as the internet users may not properly receive the notice when entering the different jurisdiction. Therefore, the protection of electronic data in cyberspace is on oversight and needs the laws to control the transactions. The General Data Protection Regulation (the Regulation), is an example of the EU legislation targeting on economic operators, including micro, small and medium-sized enterprises with regard to the processing of personal data and the free movement of that data. The Regulation with unilaterally extraterritorial effect was adopted by the European Parliament, and the European Council on April 27th, 2016 and will become binding automatically throughout the EU as of May 25th, 2018.

2. The reform of EU data protection legislation: The General Data Protection Regulation (GDPR)

---

1 Ph.D. Candidate, School of Law, Wuhan University, Hubei, China.
The General Data Protection Regulation (the Regulation)\textsuperscript{8} has replaced the 1995 Data Protection Directive (the Directive).\textsuperscript{9} The Directive which adopted on October 24, 1995, was mainly focused on the protection the fundamental rights and freedoms of natural persons, and promote the free-flowing of such data among the Member States. However, the European Commission had proposed its data protection reform in January 2012, to ensure the protection of personal data and increase in cross-border flows of such data within the Union in a digital age that is vastly different from the time in which the 1995 Directive was established.\textsuperscript{10} The Regulation focuses to the processing of personal data by a controller or processor, where the processing activities relating to the goods or services which offer to the data subjects residing or placing in the EU or the monitoring of data subject’s behavior that takes place within the EU. The Regulation proposes some new rules that will impact businesses and organizations across the globe.

The critical changes implemented in this legislation are the following components: 1. Increased territorial scope. Non-EU based businesses and organizations are caught by the Regulation in case of data subjects residing or placing in the Union or their behavior taking place within the Union (Article 3); 2. The obligation of the data processor. It has more clearly regulated the specific obligations of the data processor, such as implementation of appropriate data security measures (Article 32), cooperation with the supervisory authority (Article 31), designation of the data protection officer (Article 37); 3. Data protection officer (DPO). It is a new requirement of the Regulation that data controllers and data processors, under certain circumstances, must designate a DPO for specific tasks (Article 37-39); 4. International data transfer. The transfer of personal data is subject to the provisions which are on the basis of the adequate decision, appropriate safeguards, otherwise, the specific situations are allowed under the derogation provision (Article 42-49); 5. One-stop-shop mechanism. The lead supervisory authority is responsible for cross-border data processing operation and handles cases carried out in the EU (Recital 127);\textsuperscript{11} 6. Explicitly consent from the data subject. It should be a freely given, specific, informed and unambiguous indication by a statement or clear affirmative action (Article 4(11), Recital 32); 7. Notification. The data controllers must notify data breaches to the supervisory authority within the timeframe allowed (Article 33, Recital 85); and 8. Sanctions. The imposition of administrative fines to businesses or organizations for infringement of the provisions and non-compliance with the order by the supervisory authority is up to 20,000,000 EUR, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83).

3. The impact on cross-border business

The Regulation with extraterritorial effect mainly aims to push EU to a digital single market that boosts competitive growth, transforms EU’s industrial sector and creates new products & services for expanding market, however, it also produces legislative effect in the third countries, of course, giving impact on the cross-border trades. As the Regulation applies to all organizations or companies which process the personal data of data subjects residing in the Union, even where they were physically located outside the EU countries, hence, it gives critical effects, both opportunity, and concern to trade partners.

i. The opportunity to Trade Partners

\textsuperscript{8} The 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).

\textsuperscript{9} The Directive(EC) 95/46 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(1995).

\textsuperscript{10} Trunomi, “GDPR Key Changes”, available at http://www.eugdpr.org/key-changes.html.

The Regulation, one single European-wide set of the rules, will change the trade model at the global level. As trade recorded, The EU exports were mainly to Asia with about one-third of the total recorded in 2016. It is claimed that the EU is ASEAN’s 2nd largest trading partner accounting for around 13% of ASEAN trade while China and ASEAN represent the EU’s 2nd and 3rd largest trading partner accordingly.12 Notably, China has continued to increase its market share with the EU, and it is more than doubled in export between 2008 and 2015.13 In 2016, 20% of EU businesses reported as e-commerce sales; it was a moderate increase compared with 15% in 2010. In details, 13% of businesses reported having conducted websites or apps to sell their goods or services to customers (B2C) and 12% to other businesses (B2B).14 The Regulation is estimated to make business saving of €2.3 billion per year,15 and stimulates innovation through a number of steps such as one-stop-shop mechanism that supports companies only dealing with one single supervisory authority in the EU country in which they are mainly based. Viviane Reding, MEP and former vice-president of the European Commission who proposed the Regulation in 2012 stated that this legislation would eliminate trade barriers as companies can reach the entire European Market and enjoy a level playing field.16 This reform will enhance trust in digital services, consequently, give a real push to the digital single market for Europe’s 500 million citizens.17 She has also believed that the Regulation can create a fair competition in the globalized world when non-European companies provide goods or services to European consumers under the same rules as European companies.18

The harmonization and simplification of the Regulation are claimed as the solution to reduce burdensome for companies to conduct their businesses in the EU. The new rules can solve the problem of unnecessary additional costs occurred in the Directive which required the multinational companies’ data controllers to comply with a variety of notification and the authorization among the Member States prior transfer data to third countries.19 Under the EU data protection reform with the Digital Single Market Strategy, it is expected to contribute € 415 billion per year to EU economy and create hundreds of thousands of new jobs.20 Notably, the number of jobs that require information and communications technology skill is expected to rise by 16 million by 2020 and 90% of jobs required basic information technology skills.21

ii. The concern to Trade Partners

As the Regulation extended territorial reach, companies which targeting EU market are effectively expected to modify their entire business structure and establish internal governance schemes related to the processing of personal data to comply with EU law. The Regulation becomes enter into force on May 25th, 2018, the awareness of organizations around the world has reached by

20 Eurostat, supra note 13.
approx. 50% and 65% of those have started preparing for it.\textsuperscript{22} It is the time for organizations or companies that target EU market but physically presented outside of Europe, to start the process of ensuring its business structure compliance with the Regulation. It’s certain that there are many stakeholders in the supply chain will be caught by the Regulation, for example suppliers, manufacturers, distributors and customers, including subcontractors (stocking warehouses), outsourced services (IT support, insurance administration services), after-sale services partners (maintenance, warranty) which are involved in goods and services offering. Organizations or companies need a comprehensive rule of business model to fit the Regulation’s regulatory obligation. Furthermore, the data protection obligations require oversight and cooperation of cross-functional team with different backgrounds such as legal, sales and marketing, information technology (IT) and human resources (HR).\textsuperscript{23}

Even though the Regulation provides the single-set rule to facilitate the trade relation, the concerns of application of the Regulation are raised in some dimensions such as the costs, the trust in the privacy standards. Some arguments pointed that a non-European organization with some limited interaction with EU residents has to implement potentially costly administrative measures such as appointing a data protection officer (DPO).\textsuperscript{24} The cost burden on companies from compliance will not offset by efficiency gains even in the long run.\textsuperscript{25} The mentioned costs are notably from the obligation regarding designation a representative in the EU in case of the data controller or processor not established in the EU (Article 27), implementation of Data Protection Impact Assessment (Article 35-39, Recital 84,90-95), designation of Data Protection Officer (Article 13-14,35,37-39, Recital 77), and Notification of Data Breach (Article 33-34,40, Recital 73,85-88). Other challenges are including the shortage of the professional data protection officer (DPO),\textsuperscript{26} the risk of enforceable sanctions, the behavior of data controllers,\textsuperscript{27} the supervisory authority dealing with the questions regarding the administrative fines.\textsuperscript{28}

\textit{iii. The key actions}

According to the obligation regulated in the Regulation, cross-border businesses have to evaluate the external and internal conditions, including the market potential, internal business structure, the data security, the pros and cons of new procedures. The key actions for the EU market are proposed as in the following issues: 1. review their business structure in the whole system and find out which parts are caught by the Regulation; 2. Implement the likelihood of risk assessment to identify some risks which may give the effect to business and customers; 3. appoint the representative in the EU in case of controllers not established in the EU; 4. assign the data controllers and the representatives as the contact point to work closely with supervisory authorities and share the best practices or problems in practice; 5. implement training programs for cross-functional teamworks; and

\begin{itemize}
\item \textsuperscript{22} Eduard Meelhuysen, “The Final Analysis: What you need to know about the EU GDPR Legislation”, Cloud Industry Forum, available at https://www.cloudindustryforum.org/content/final-analysis-what-you-need-know-about-eu-gdpr-legislation
\item \textsuperscript{26} DLA PIPER, “EU General Data Protection Regulation – Key Changes”, available at https://www.dlapiper.com/en/us/focus/eu-data-protection-regulation/key-changes/
\item \textsuperscript{27} Christopher Kuner, “Extraterritoriality and regulation of international data transfers in EU data protection law”, International Data Privacy Law, Vol. 5, 2015, at p. 235.
\item \textsuperscript{28} P. Galdies, “A Summary of the EU GDPR Data Protection Regulation”, DataIQ, 2016, available at https://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation
\end{itemize}
6. implement periodic review to ensure the whole system of processing of personal data is in compliance with the Regulation.

4. Conclusion

The reform of EU data protection legislation with extraterritorial effect will give a big change of business model, notably, dealing with the processing of personal data across the border. The Regulation poses a new challenge to the EU’s trade partners in term of the complexity of the cyberspace and more stakeholders involved. The Commission has promoted the mechanisms to facilitate the effective enforcement of the Regulation. However, it is not only the public sectors of the state but also the private sectors such as international organization, non-governmental organization, especially, multinational companies will play a greater role as they give the big impact to the economy. Under the different of legal systems and business environment, the key point is to balance the various interests involved among countries. The Regulation not only provide the market opportunity to trade partners in term of rules harmonization, but also pose the challenges to the stakeholders to design its business model in order to enhance their market competitiveness in the EU. Therefore, identifying and understanding the Regulation's extraterritorial effect and the implication remain significant challenge. Third countries and non-EU companies, in response to this legislation, may actively engage with the EU in sharing experiences and establishing a regulatory structure for cross-border data flow in full compliance with and without prejudice to the EU data protection law.