Routledge
Taylor & Francis Group

Journal of Global Information Technology Management

ISSN: 1097-198X (Print) 2333-6846 (Online) Journal homepage: www.tandfonline.com/journals/ugit20

The Impact of GDPR on Global Technology Development

He Li, Lu Yu & Wu He

To cite this article: He Li, Lu Yu & Wu He (2019) The Impact of GDPR on Global Technology Development, Journal of Global Information Technology Management, 22:1, 1-6, DOI: 10.1080/1097198X.2019.1569186

To link to this article: https://doi.org/10.1080/1097198X.2019.1569186

JOURNAL OF GLOBAL INFORMATION TECHNOLOGY MANAGEMENT
2019, VOL. 22, NO. 1, 1–6
https://doi.org/10.1080/1097198X.2019.1569186

The Impact of GDPR on Global Technology Development

He Li[a], Lu Yu[a], and Wu He[b]

[a]School of Management, Jilin University, Jilin, P. R. China; [b]Department of Information Technology and Decision Sciences, Old Dominion University, Norfolk, VA, USA

ABSTRACT

The European Union's General Data Protection Regulation (GDPR) demands significant data protection safeguards and poses both new challenges and potential opportunities to organizations around the world. Most organizations are not yet adequately prepared for compliance with the GDPR. To minimize liability under the GDPR, organizations around the world need to make changes to be in compliance with the GDPR. This editorial preface discusses GDPR's impact on global technology development including both challenges and opportunities. Furthermore, we discuss how China and the U.S., the two leading global economic power, can better respond to the challenges and opportunities brought up by GDPR.

KEYWORDS

General Data Protection Regulation (GDPR); privacy compliance; cybersecurity; technology development; data governance; risk management; personal data

Introduction

General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, is a data protection legislation which lays down rules for processing, storing, managing data from people who are currently within the European Union(EU, 2016). This new legislation strengthens EU's data protection to meet the new privacy challenges brought by the development of digital technologies. While the GDPR only protects EU citizens, its impact is bound to be global in nature, affecting any organization that targets the European market or provides services and hold personally identifiable information on EU residents. GDPR gives consumers a high degree of control, such as the right to withdraw consent (Art.7), to be forgotten (Art.17). At the same time, high requirements are put forward for data controllers and processors, including data protection by design and by default (Art.25), recording all processing activities (Art.30). GDPR says that organizations should get user consent to collect data and "implement appropriate technical and organizational measures" to protect personal data of EU residents (Kaushik & Wang, 2018).

Organizations that process data related to EU residents will be held accountable for non-compliance with GDPR. In particular, GDPR poses both a new challenge and a potential opportunity for technology companies, cloud service providers, data center providers and marketers which will have to adopt stricter security measures, standards and processes to protect, process and manage personal data to ensure their compliance with GDPR. Otherwise, they will likely to receive potentially large fines from the EU. GDPR defines personal data as anything that can be used to identify an individual person. This includes personally identifiable details such as names, email addresses, social security number, IP addresses, telephone numbers, location data, birth dates as well as other information related to genetic, economic, cultural or social identity. Large technology companies like Google, Facebook, and Amazon have already updated their privacy policies and practices to comply with the GDPR. The organizations which are compliant with GDPR will likely have a competitive advantage over their competitors who are not compliant.

CONTACT Wu He whe@odu.edu Department of Information Technology and Decision Sciences, Old Dominion University, Norfolk, VA 23529, USA

Given the global impact of GDPR, this editorial preface aims to discuss its impact on global technology development. As many online and newspaper articles have discussed the general impact of GDPR on business, this essay particularly focuses on the challenges and opportunities GDPR has brought about on technology development in the United States and China, the two leading global economic powers.

Impact on Technology Platforms

GDPR is expected to have a significant impact on the technology platforms and data architectures that currently collect, store and manage personal data (Mackay, 2017). Since GDPR has high requirements for data controllers and processors to handle personal data including data protection by design and default, and recording all processing activities, organizations will have to conduct a thorough internal assessment for their technology platforms and data architecture including various information systems, websites, databases, data warehouse and data processing platforms in order to better understand what personal data was collected and where personal data exists. After the internal assessment, organizations will likely have to make changes to their technology platforms and data architecture in order to meet GDPR's requirements. In some cases, reengineering of existing systems or platforms will be needed to reduce the risk of non-compliance with GDPR.

GDPR also requires organizations to offer EU residents robust privacy rights such as Right to be Forgotten, Right of Access to Data, Right to Data Portability, and Right to Explanation of Automated Decision-Making (Kaushik & Wang, 2018). If a user wants to find out what personal data a company has collected about him or her and for what purpose, this user can request the company to provide an answer in a timely manner (Right of Access to Data). It is possible that a large company such as Amazon and Alibaba could receive thousands of requests from their customers about how the company is using their personal data every day. If the customer is not satisfied with the way the company handles his/her personal data, the customer could ask the company to delete the personal data (Right to be Forgotten). Furthermore, companies that have employees living in the EU or from the EU also need to handle their employees' personal data such as photos, bank details, tax and pension details, health and safety reports, sickness records and medical information, CVs, job application forms, disciplinary procedures, holiday requests and salary information (Beacham, 2018). To meet the request of customers or employees for efficient access to their personal data and to remove personal data from the system efficiently, the company may have to refine or reengineer their existing platforms and systems. Specifically, first the company needs to identify personal data related to this customer or employee from all sources such as customer relationship management system, human resource management systems, databases and archives. Second, the company needs to implement holistic search tools that can search across all technology platforms, systems, archives and architectures to identify and extract personal data relating to individuals (Mackay, 2017). Without holistic search tools, there is no guarantee that the company will be able to ensure that all the personal data associated with an individual customer or employee can be handled appropriately.

To meet the requirements of GDPR, companies need to invest a lot of manpower and resources on upgrading their technology platforms, updating privacy policies, changing advertising practices and adjusting data storage and processes, etc. The impacts on American and Chinese companies are especially significant, since the U.S. and China, the two leading global economic powers, have many companies that do business with the EU. According to the PricewaterhouseCoopers survey, 68% of American companies are expected to spend between $1 million and $10 million to meet the GDPR requirements, and 9% are expected to spend more than $10 million (PwC, 2017). Such a high cost will eventually be passed on to consumers, and thus weaken the competitive advantage of Chinese and American enterprises. Besides, GDPR is likely to be a tool of European commission to accuse non-EU companies including Chinese and American companies of having problems in data protection and then block their pace of investments and mergers.

Some Chinese and American Companies have tried to comply with GDPR. For example, Huawei, the Chinese telecommunications giant, has appointed data protection officers; and YouTube has stopped supporting third-party advertising services on reserved buys in Europe after May 21, 2018. Unfortunately, something that we don't want is also happening. Yeelight, a large smart lighting device company in China, announced that it would no longer provide services to European users Facebook and its subsidiaries WhatsApp and Instagram, as well as Google, were immediately sued just hours after GDPR came into effect for their "forced consent". These cases reflect the fact that foreign companies' business activities with the EU have already been heavily influenced by GDPR.

Impact on Cybersecurity

GDPR is expected to have implications on organizations' cybersecurity policy and practice since it requires companies to implement reasonable data protection measures to protect consumers' personal data and privacy against data loss or exposure. Article 5 of the GDPR summarizes some of the key privacy and data protection requirements such as requiring the consent of subjects for data processing, anonymizing collected data to protect privacy, providing data breach notifications, safely handling the transfer of data across borders, and requiring certain companies to appoint a data protection officer to oversee GDPR compliance. Since many cybersecurity incidents and data breaches have occurred in the past, GDPR now requires the data controller to "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." Thus, companies need to step up their cybersecurity efforts to protect against threats and breaches and to minimize liability under the GDPR. GDPR will further increase the demand for cybersecurity professionals and data protection officers. To address the current skills shortage for cybersecurity professionals and data protection officers, both governments and technology companies will need to invest in more cybersecurity training and education programs (Withey, 2018).

The GDPR's high requirement for securing personal data also brings a new opportunity to companies. Privacy and security issues are often accompanied by user trust, which is one of the important issues in modern business. In recent years, scandals about personal data security vulnerability and cases of how companies unproperly use and sell information they collect from their consumers have aroused general concern and led to negative impact on consumer trust (Midha, 2012). Capgemini's report shows that 39% of consumers will spend more when they are convinced that an organization protects their personal data (Capgemini Research Institute, 2018). In other words, gaining consumer trust around data privacy and security could lead to more sales and translate into competitive advantage (Conroy, Narula, Milano, & Singhal, 2014). Chinese and US companies should seize the opportunity to enhance their capabilities for protecting personal data so that they can not only minimize the legal liability of GDPR but also win the trust of consumers and create a unique competitive advantage over those who cannot be in full compliance of GDPR.

Impact on Emerging Technologies

We believe that GDPR will have significant impacts on the development of emerging technologies. As we know, emerging technologies such as artificial intelligence, block chains and cloud computing are effective means of boosting performance and productivity. The development and application of these emerging technologies are key to promote the economy and have become one of the strongest competitive factors among countries. But it should be noticed that these technologies deliver their value through massive data and high-quality algorithms. Stricter regulations on data handing and processing are likely to inhibit new technology development and use, and will inevitably increase the cost to develop new technologies.

GDPR will affect the development of Artificial Intelligence (AI) applications by increasing the costs and limiting the application scope. Article 13 and 22 of GDPR require that certain algorithm

decisions need to be reviewed and explained by humans, and such restrictions will greatly increase labor costs and break the inherent balance between accuracy and transparency; Article 17 provides user with erasure of personal data without undue delay, which might destroy key rules underpinning the AI system, and thus resulting in a decrease in the efficiency and accuracy of algorithms, or even breaking it entirely. As to blockchains, it is difficult to identify the data controller and hard to require each node to perform strict obligations (Wallace & Castro, 2018). Furthermore, as the data of each node of the block chain affects subsequent records, if blockchain users have the right to delete and correct data (as stipulated in articles 16 and 17 of GDPR), then the efficiency and effectiveness of blockchain will cease to exist. With regard to cloud computing, GDPR creates obligations for cloud platform service providers, who will be required to provide information about all intended processing to data subjects pursuant to Articles 13 and 14. This will definitely bring operational difficulties and increase the cost of operating a cloud platform, as the efficiency of cloud computing comes from optimal resource allocation which is determined by current tasks and cannot be fully determined at the time of data collection.

Although many Chinese and American companies are obligated to comply with GDPR, the EU companies are still the most affected in the field of emerging technologies since they mostly deal with personal data of EU residents. If the EU emerging technology industry cannot effectively solve the above-mentioned restrictions by means of significant technological upgrading, which seems to be unlikely in the short term or in other ways, the development and application of emerging technologies within the EU will slow down significantly. Many other relevant industries, such as credit cards, e-commerce, as well as intelligent manufacturing, which are supported by those emerging technologies, will also be significantly affected. In contrast, Chinese and U.S. companies will be less hindered in improving and applying these emerging technologies than EU companies since they can create products that serve their domestic consumers. In the long run, Chinese and U.S. companies may develop stronger competitive advantage over EU companies in the area of emerging technologies.

Recommendations

Given the universal and significant impact of GDPR, we believe that China and the United States should actively respond to those challenges and opportunities. Although many Chinese and American companies are not necessarily required to follow GDPR strictly, considering that privacy protection is an inevitable requirement for future development and an important way to maintain competitiveness, we believe that all organizations should take GDPR as a benchmark to gradually improve their privacy protection awareness and capabilities. This editorial puts forward the following recommendations.

Focusing on Improving Privacy Protection Methods

China and the United States should seize their advantages with emerging technologies to explore more secure and efficient data processing methods to enhance their capabilities to protect personal data. For example, it can focus on improving privacy and personal data protection methods such as optimizing anonymization methods and data mining algorithms to solve the contradiction between transparency and efficiency. In addition to technical means, organizational measures also need to be explored and learned from practice. For example, what methods are needed to measure and bridge the gap that a business has to cross in order to achieve compliance with GDPR? How to estimate the cost of implementing GDPR within a company? Fortunately, the Data Protection Impact Assessment required by GDPR is a good way to test new technologies on privacy protection.

Paying Attention to Trust Building

Obviously, for those companies which have commercial or scientific relationship with the EU, increasing user trust can greatly reduce GDPR-related complaints. Moreover, showing transparency

and honest privacy practice to users is an effective way to improve trust and reputation. Companies around the world need to step up their efforts in privacy risk management and protection of personal data in order to survive or remain competitive in the EU market.

Conclusion

The GDPR will have a massive impact on future technology development. Those who can adapt to meet GDPR requirements will succeed in the future and those who cannot will eventually fail (Wright, 2017). Although this editorial has discussed many potential challenges of GDPR, we encourage companies to think of compliance with GDPR as a strategic opportunity for gaining a competitive edge in this data-driven world. Technology companies that target global markets are recommended to step up their efforts to secure their data, systems, products and services for compliance with GDPR. We also encourage scholars and practitioners to study issues related to the implementation and compliance of GDPR and share insights. IS and IT have the potential to help in many important areas. For example, IS scholars can propose frameworks, methods and architectures that meet GDPR's requirements for revoking consent and permanently deleting widely disseminated personal data (Politou, Alepis, & Patsakis, 2018), estimate the cost to achieve compliance with GDPR, identify various factors that affect the compliance with GDPR, investigate how culture and national conditions influence the implementation and compliance of GDPR, and explore the impact of GDPR on operations and financial performance.

Notes on contributors

He Li is a Professor and Chair of the Department of Information Management, School of Management at Jilin University, China. Her research interests include information and knowledge management, information behavior, security and privacy, information system development and analysis, e-commerce user information development, and innovative community management. Her research has been funded by the National Development and Reform Commission, the Ministry of Science and Technology, and other enterprises in China.

Lu Yu is a third-year graduate student at the School of Management, Jilin University, China. Her research interests include information security and privacy, and information behavior. Her work has been published in *Journal of The China Society for Scientific and Technical Information*. She has presented papers and been invited as anonymous reviewer of *International Journal of Information Management*, and *Behaviour & Information Technology*.

Wu He is an Associate Professor of Information Technology at Old Dominion University, Norfolk, VA, USA. His research interests include Data Mining, Information Security & Privacy, Social Media, Knowledge Management and Computing Education. His research has been funded by NSF, NSA, NASA and other organizations. He has published over 80 journal articles in such outlets as *Information & Management, Journal of the Association for Information Science and Technology, International Journal of Information Management, and IEEE Transactions on Industry Informatics*.

References

Beacham, J. (2018). Is your practice GDPR ready? *In Practice*, *40*(3), 124–125.

Capgemini Research Institute. (2018). Seizing the GDPR advantage: From mandate to high-value opportunity. Retrieved from https://www.capgemini.com/wp-content/uploads/2018/05/GDPR-Report_Digital.pdf

Conroy, P., Narula, A., Milano, F., & Singhal, R. (2014). Building consumer trust - Protecting personal data in the consumer product industry. Retrieved December 21, 2018, from https://www2.deloitte.com/insights/us/en/topics/risk-management/consumer-data-privacy-strategies.html

European Union. (2016) General data protection regulation. Off J Eur Union 49: L119. Retrieved from https://gdpr-info.eu

Kaushik, S., & Wang, Y. (2018, December 20). Data privacy: Demystifying the GDPR. Retrieved from https://ischool.syr.edu/infospace/2018/05/25/data-privacy-demystifying-gdpr/

Mackay, D. (2017). The impact of GDPR from a technology perspective – is your platform ready? Retrieved December 20, 2018, from https://www.ness.com/11101-2/

Midha, V. (2012). Impact of consumer empowerment on online trust: An examination across genders. *Decision Support Systems*, *54*(1), 198–205. doi:10.1016/j.dss.2012.05.005

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1), tyy001. doi:10.1093/cybsec/tyy001

PwC. (2017). Pulse survey: US companies ramping up General Data Protection Regulation (GDPR) budgets. Retrieved from https://www.pwc.com/us/en/services/consulting/library/gdpr-readiness.html

Wallace, N., & Castro, D. (2018). The impact of the EU's new data protection regulation on AI. Retrieved from https://www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/

Withey, V. (2018, December 20). The impact of GDPR on the technology sector. Retrieved from https://gdpr.report/news/2018/03/19/the-impact-of-gdpr-on-the-technology-sector/

Wright, T. (2017). The impact of GDPR on marketing technology and cybersecurity. Retrieved December 22, 2018, from https://martechtoday.com/impact-gdpr-marketing-technology-cybersecurity-201635