Review Paper
Informatization Policy Vol. 27, No.3 (2020), pp.003-018
https://doi.org/10.22693/NIAIP.2020.27.3.003

The Effects of GDPR on the Digital Economy: Evidence from the Literature

Aryamala Prasad* · Daniel R. Pérez**

Abstract In the growing digitalized world, the European Union implemented the General Data Protection Regulation(GDPR) to establish a comprehensive data protection framework across member states. Given the constitutional roots of GDPR, the EU's regulatory approach is different than other data protection regimes. The new regulation has strengthened individual rights to data protection, but it also introduced several obligations for businesses that collect and process personal data. We review the existing literature on privacy, particularly GDPR, from a policy perspective. The evidence outlines data regulation's effects on competition, innovation, marketing activities, and cross-border data flows. The discussion highlights the tradeoffs between increased regulation of data protection and its effects on the market.

Keywords : GDPR, regulation, data protection, privacy, digital economy

GDPR이 디지털 경제에 미치는 영향: 문헌 자료에 근거하여

아라말라 프라사드* · 다니엘 페레즈**

요약 전세계적으로 디지털 전환이 확산됨에 따라 유럽연합(EU)은 회원국 간의 포괄적인 데이터 보호 프레임워크를 구축하기 위해 GDPR(General Data Protection Regulation)을 시행하였다. GDPR의 헌법적 뿌리를 고려할 때, EU의 규제 접근법은 다른 데이터 보호 규정들과는 차이가 있다. GDPR은 데이터 보호에 대한 개인의 권리를 강화하였다. 하지만 개인의 데이터를 수집하고 처리하는 기업에 대한 몇 가지 의무 또한 도입하였다. 본 연구에서는 정책적 관점에서 프라이버시, 특히 GDPR에 관한 기존의 문헌을 고찰하였으며, 이를 통해 데이터 규제가 경쟁, 혁신, 마케팅 활동 및 국경을 초월한 데이터 흐름에 미치는 영향을 개략적으로 리뷰 하였다. 그리고 본 연구는 프라이버시와 GDPR이 시장에 미치는 영향 사이의 절충안을 강조한다.

주제어 : GDPR, 규제, 데이터보호, 프라이버시, 디지털경제

Received Aug 26, 2020; Revised Sep 11, 2020; Accepted Sep 14, 2020
* Corresponding author, Regulatory Studies Center, Trachtenberg School of Public Policy and Public Administration, George Washington University. (aprasad1@gwmail.gwu.edu)
** Regulatory Studies Center, Trachtenberg School of Public Policy and Public Administration, George Washington University. (danielperez@email.gwu.edu)

Ⅰ. Introduction

The European Union(EU) introduced the General Data Protection Regulation(GDPR) to establish a comprehensive data protection framework across its member states—replacing the existing Directive 95/46/EC. The modernized law, enforced in May 2018, operates in the context of the ubiquitous and globalized nature of personal data to maintain the EU's commitment to providing data protection as a fundamental right. Accordingly, the regulation places new limits on businesses that use personal data to offer products and services.

The monetary value of personal data increases the significance of GDPR. Although many countries have data protection or privacy regulations, the extra-territorial jurisdiction of GDPR expands its scope across the world. Any business that collects data on EU residents must adhere to the law. Therefore, the regulation has global implications for the data economy worth $3 trillion(Thirani & Gupta, 2017). Personal data adds value by assisting companies in customizing products, understanding market trends, and creating targeted advertising to increase revenues and improve existing services(Spiekermann, et al., 2015). Social media services are offered for free because the user-generated data serves as a prized possession for targeted advertising. However, the regulatory requirements involving GDPR adds filters to the flow of personal data with the goal of limiting its potential misuse by requiring increased transparency and accountability in the collection and processing of personal data.

However, these same regulatory requirements can potentially alter the performance of markets in substantive ways. For instance, compliance costs can disproportionately affect small- and medium-sized businesses. New limits on collecting and processing personal data may shift incentives and push companies to abandon certain business models while pursuing others. Regulation may result in fewer mergers or reduced investment because of the constraints associated with data transfer between companies and countries. The academic literature on policy and regulation, which spans across a range of disciplines such as economics, marketing and law, has attempted to better understand the influence of GDPR on markets.

Against this background, we review the existing literature on GDPR from a policy perspective. Most of the articles focus on the effect of GDPR on the digital economy. In particular, the following major research themes emerge from our survey: compliance costs of GDPR; the effects of data regulation on competition, innovation, marketing activities, and cross-border data flows. The discussions highlight how limits place by GDPR on the use of personal data affect market outcomes. Given the continued debates on the tradeoffs between privacy and its effects on the market, we begin by explaining the genesis of GDPR, its requirements, and compare it to competing global data protection regulations to contextualize the new legislation.

Ⅱ. Literature Review

1. General Data Protection Regulation

The European data protection law is rooted in

the normative perspective of privacy and data protection as human rights(Hoofnagle, et al., 2019). The EU Charter of Fundamental Rights grants individuals the right to the protection of personal data. Previously, Directive 95/46/EC offered data protection guidelines but left the enactment to individual member states. Uneven implementation of data protection across the EU made it challenging for businesses to ensure compliance in different countries. Further, the impact assessment by the European Commission(EC) stated that rapid technological developments and globalization necessitated a stronger data protection framework(European Commission, 2012). Therefore, the new legislation's objectives include improving user control over data and standardizing data protection law in 27 member states to promote the free flow of information within the EU single market.

Unprecedented growth in personal data collection and processing by private and public authorities has increased the risks to EU citizens' individual rights. The European Commission observed that the Internet has facilitated global data flows without ascertaining adequate data protection in other countries European Commission, 2012). Further, individuals are often not aware of the purpose of collecting and processing their data are processed. The EC's *ex-ante* Impact Assessment noted that before GDPR, only 41 percent of data controllers maintained or updated privacy policy notices while 70 percent of individuals were concerned about their personal data being processed differently than its originally intended purposes(European Commission, 2012).

From an economic perspective, the EU was concerned about fragmented data protection laws in across its member states. Uneven implementation of the Privacy Directive resulted in an estimated administrative burden of 2.9 million euros per year within the EU internal market(European Commission, 2012). The regulatory compliance cost for large multinational companies was estimated at 2.5 million euros per year, and the EC found it was more challenging for small and medium businesses to comply with the complex and fragmented data policies within EU member states.

To address these problems, the EU introduced GDPR to establish a comprehensive data protection framework and harmonize rules within the EU common market. It defines personal data as any information relating to "an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"(GDPR, 2016). Mainly, the regulation strengthens individuals' right to: access, amend, and erase their personal data; restrict sharing or processing of information by third parties; request their personal data in machine-readable format that is portable to another company/organization; object to the processing of data for profiling or direct marketing purposes including for research; request companies not to rely solely on automated algorithms for decision-making.

The regulation also allocates specific responsibilities to businesses to safeguard personal data. Seven key principles drive these obligations: lawfulness, fairness and transparency; purpose limitation;

data minimization; accuracy; storage limitation; integrity and confidentiality, and accountability. Together these principles are intended to ensure that data are used and processed for intended purposes only. The regulation also classifies businesses as "data controllers" and "data processors" to establish accountability. The data controller refers to businesses that gather data directly from consumers to fulfill a contractual obligation. Companies that use personal data on behalf of a data controller are called data processors—they assist the controller rather than engaging directly with data subjects.

Specifically, companies must take the following steps. First, they must inform consumers how organizations will use their data, and they must obtain explicit consent to process them. The regulation underscores the importance of freely-given and informed consent. In the context of online data collection, it means that websites have to seek opt-in consent rather than the default opt-out option to decline website tracking. Second, businesses must implement technical and organizational measures to ensure that only information needed for specific purposes is collected(purpose limitation) and only stored until necessary(data minimization). Businesses must also take steps to reduce third-party access to data. Third, businesses have to record all processing activities. Fourth, data must be maintained in a format that enables the transfer or deletion of data upon individuals' requests(Theodorakis, 2018). Fifth, organizations must implement security measures to ensure the confidentiality of user data and must provide notification of any data breach within 72 hours. Businesses are also tasked with appointing a Data Protection Officer(DPO) to monitor that data processing and transfer are GDPR compliant. Lastly, an annual Data Protection Impact Assessment must be conducted to identify and minimize data protection risks particularly when collection or processing of data uses new technologies, tracks particularly sensitive data(like location data or religious beliefs), involves the use of automation to make decisions with potential legal effects, or is collected from particular classes of data subjects(e.g., children) (GDPR, 2016a).[1)]

The regulation imposes additional requirements on companies that collect user data. Any personal information gathered from customers can be shared with data processors only to fulfill a contractual obligation. More importantly, data controllers must guarantee that processors are GDPR compliant. For instance, a retail website collecting credit card information can use that data to process payments. Nonetheless, it cannot share that information for advertising purposes without the informed consent of the user. Furthermore, the user must be informed of how the data will be processed. As a result, GDPR compliance goes beyond the first point of data collection and imposes costs on third parties. Additionally, any cross-border processing of data requires that the receiving country has adequate protections.

Enforcement actions are taken by each member state's Data Protection Authority(DPA) which can

1) https://gdpr.eu/data-protection-impact-assessment-template/

fine organizations it finds as failing to comply with GDPR's requirements "up to $20 million or 4 percent of annual revenue, whichever is higher"(GDPR, 2016a). It also introduces a one-stop-shop mechanism to allow the DPA where the main company is established to enforce the regulation across EU member states. Interestingly, GDPR does not use revenue or businesses size thresholds to limit the scope of regulated entities(Hoofnagle, et al., 2019, 73).

While the requirements increase the protection of personal data, they also disrupt the personal data value network. Enforcing GDPR leads to restrictions on data processing, thereby substantively limiting certain economic activities(Cave, et al., 2012). Implementing new requirements can increase the costs of products or services to customers and change the incentives to continue some activities. These shifts have serious implications for market outcomes.

2. International Regulation of Data Protection

The GDPR implements extraterritorial reach in the enforcement of its data protection regime, and the EU accounts for a considerably large share of the international market in information and communication technology(ICT). These facts are notable given that scholars have recognized the EU's history of successfully diffusing its regulatory policies abroad—particularly among other countries within the Organization for Economic Cooperation and Development(OECD). This is what Bradford(2012) describes as the "Brussels Effect." Countries interested in maintaining access to the EU market for personal data can either comply with GDPR or secure approvals for transferring data between jurisdictions which include having the EC issue a determination that their existing regulatory regime provides a similar level of protection to GDPR—called an "adequacy decision."[2] Interestingly, the EC had only recognized six OECD member countries as providing an adequate level of protection, while adequacy talks remain ongoing with South Korea.[3] Most recently, the European Court of Justice(ECJ) struck down a mutual recognition framework called "Privacy Shield" that allows commercial data flows with its largest trading partner in ICT, the United States(U.S.)[4] The ECJ ruled that existing U.S. national security laws enabling government surveillance violated the privacy and data protection rights of EU citizens.

Given GDPR's implementation in 2018, policymakers in other countries can consider a range of alternative regulatory approaches to data protection and inform their deliberations with empirical evidence of the effects of GDPR versus other approaches. In short, there exists an opportunity for international regulatory competition in the adoption of data protection regimes(Chander, et al., 2019). The following

2) Article 45 of Regulation (EU) 2016/679.
3) Businesses operating in other countries can also transfer data between EU and non-EU countries if they sign an EC legal document called a "standard contractual clause." https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents
4) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

section describes the regulatory approach of the EU's largest trading partner in ICT(outside of intra-EU data flows)—the U.S.—before turning to recent evidence of GDPR's effects.

3. The U.S. Consumer Protection Approach to Privacy and Data Protection

Whereas GDPR is an omnibus data protection regime centered on corporate governance(Jones and Kaminski 2020) intended to implement constitutionally-guaranteed, positive rights to EU citizens(McGeveran, 2016), the U.S. implements privacy laws based on a "notice-and-choice" approach(Chander, et al., 2019) with narrower, sectoral data protection regimes applicable only to particular kinds of data and industries(i.e., medical providers' use of health information).

The regulator of data privacy at the national (federal) level is the Federal Trade Commission (FTC)—which uses a consumer protection framework that regulates the relationship between businesses and consumers by taking enforcement actions against businesses found to employ "unfair and deceptive practices"(UDAP). States attorneys general also take enforcement actions related to privacy and data protection at the state level under similar UDAP frameworks protecting consumers "in direct relationships with companies"(Jones & Kaminski, 2020). Notably, the FTC's criteria for determining whether practices are "unfair" and "deceptive" are broadly applicable to all industries(i.e., the FTC does not have a narrow mandate to regulate data protection or privacy). Relatedly, unlike the GDPR, the U.S. does not currently have data protection regulations that grant individuals a private right of action against businesses.[5] With very few exceptions at the state level, only the FTC and states attorneys general can bring enforcement actions against companies.[6]

Although several U.S. states have passed data protection legislation with many principles similar to GDPR, such as a focus on transparency and privacy by design, they still rely on a traditional, U.S. consumer protection approach which results in a much more narrow scope vis-à-vis GDPR. For instance, the California Consumer Privacy Act(CCPA) grants similar rights contained in GDPR(e.g., the right to request deletion, the right to opt-out of businesses selling data), but they only apply to consumers' direct relationship with businesses(Hoofnagle, et al., 2019). Furthermore, CCPA applies only to for-profit businesses operating above certain revenue thresholds or that handle the personal information of at least 50,000 California residents.[7] In general, unless businesses are prohibited by sectoral laws from processing or collecting certain data, CCPA presumes the data collection is valid(Chander, et al., 2020; Hoofnagle, et al., 2019)—eschewing GDPR's more precautionary approach, where specific conditions must exist(and in some cases require explicit approval) for data collection and processing to occur.

5) Several states have proposed legislation to this effect, and California recently implemented the California Consumer Privacy Act.
6) For example, California's data protection regime (the California Consumer Privacy Act) allows for individuals to assert a private right of action in certain cases related to data breaches of highly sensitive financial information.
7) California Consumer Privacy Act https://oag.ca.gov/privacy/ccpa.

〈Table 1〉 EU vs U.S. Approaches to Regulation of Privacy and Data Protection
〈표 1〉 EU vs 미국의 프라이버시 및 데이터 보호 규제 접근

	EU	U.S.
Constitutional approach	Positive rights: on the list of fundamental (human) rights and services guaranteed by the state	Negative rights: restrictions on the government
Regulatory regime	Ex ante; Omnibus; Corporate governance	Ex post; Sectoral; Notice-and-consent
Regulatory Protections	Command-and-control Specific statutory authority regarding data protection/privacy Protections "follow the data"	Regulation of "unfair and deceptive practices" No specific statutory authority with the exception of sectoral data protection regimes Apply to first-party consumer-to-business relationship
Enforcement	Data Protection Authorities at the Member state level; Member states add variation in implementation via national legislation	Federal level: Federal Trade Commission State level: states attorneys general States can create additional regimes via legislation

Finally, although closer to GDPR than the status quo, CCPA does not impose any of the EU's command-and-control regulations for handling personal data including: purpose limitation, data minimization, data retention limits, recordkeeping requirements regarding data collection and retention practices, or requirements to perform privacy impact assessments(Chander, et al., 2020). Additionally, CCPA's definition of personal data is narrower in scope than GDPR.[8] The aforementioned lack of command-and-control, corporate governance mandates contained within GDPR are both theoretically and empirically relevant to our subsequent discussion of the short- and long-term effects of GDPR. The EU data protection regime prizes first-party relationships over third-party uses of data, by design, and it creates disproportionate barriers in the form of higher operating costs for certain business models—like big data or AI(Hoofnagle, et al., 2019).

Although a comparison of the EU and U.S. regulatory regimes illustrate substantive differences in both legal traditions and institutional design, it may be too early to stipulate the extent to which they necessarily produce substantively different outcomes. For example, McGeveran(2016) conducted a case study comparing Irish and American regulatory enforcement actions

8) For instance, public data are not covered.

against Facebook in 2011. He posited that both the FTC and Ireland's Office of Data Protection Commissioner reached similar enforcement outcomes regardless of their "considerably divergent bodies of substantive law." He makes the case that both agencies engaged in responsive regulation(Ayres & Braithwaite, 1992), which he argues is particularly suited for regulating industries with rapid technological changes—given the focus on dialogue rather than rigid, command-and-control approaches(McGeveran, 2016). Additionally, EU Member States often create substantive variation in the application of GDPR within their jurisdictions as a result of national implementing legislation; in the absence of an omnibus U.S. data protection scheme preempting state legislation, U.S. states are also legislating in substantively different ways. In short, these contextual differences in application present an opportunity for empirical assessments of the policy outcomes of divergent approaches to the regulation of privacy and data protection.

4. GDPR's Effects on the Digital Economy

Given the broad scope and procedural mandates contained within GDPR it is unsurprising that its implementation would substantively affect the continuously-evolving digital economy(Zarsky, 2017). Similar to its privacy-by-design features, in many ways GDPR is a deliberate effort to transform markets, by design. For instance, Jones and Kaminski(2020) point out that GDPR "explicitly attempts to influence both technological development and organizational infrastructure." Hoofnagle, et al.(2019) reference GDPR's principles of data minimization and purpose limitation, noting that these approaches purposefully generate barriers in the use of certain business models such as the use of Big Data or Artificial Intelligence(AI). Empirical evidence suggests that GDPR has affected markets with regards to compliance costs, firm competitiveness and market concentration, marketing activities, and cross-border data flows. Although more difficult to measure, GDPR is also likely influencing innovation in the digital economy due to its effect on the entry and exit of new, high-growth firms in technology sector(Acemoglu, et al., 2017, Foster, et al., 2018), while disproportionately increasing compliance costs for certain business models—such as AI, Big Data, or cloud computing. Interestingly, the European Parliament's Directorate General for Internal Policies published a review in 2012 finding that GDPR would likely affect economic competitiveness and innovation to a greater extent than what was originally estimated in the regulation's accompanying Impact Assessment (Cave, et al., 2012).

5. *The Direct Costs of Compliance*

Implementing GDPR requires businesses to invest in several resources. As mentioned earlier, the regulation tasks businesses with specific obligations. Accordingly, companies have to invest in new technologies, update their privacy policy, audit data processing flows, change storage practices, and potentially hire new personnel(Li, et al., 2019). Studies suggest a high cost of compliance, particularly for businesses outside the EU. A PricewaterhouseCoopers

survey estimated that 68 percent of American companies might spend between $1 million and $10 million(Li, et al., 2019). Recent assessments indicate that an average U.S. Fortune 500 firm paid $16 million. Compliance costs are also high in Europe: medium-sized companies spent close to $3 million in 2017-2018 to fulfill the regulatory requirements(IAPP, 2018).

In addition to investing in technological changes businesses also face costs associated with the increases in human resources. Fulfilling responsibilities under the GDPR necessitates hiring legal experts and data protection officers(Ciriani, 2015). In a 2019 survey, seventy percent of companies reported an increase in staff working on GDPR compliance.

An increase in compliance costs might also affect production costs(Christensen, et al., 2013). One estimate suggests implementing GDPR requirements can increase annual IT spending by 20 percent in some sectors. Christensen, et al.(2013) predict a decrease in labor demand by 0.3 percent in the EU. However, we could not find any recent analysis of the effect of GDPR on labor demand in the EU.

6. *Competitiveness and Market Concentration*

Empirical research in economics has mainly focused on GDPR's effect on competition and market concentration, particularly in data-intensive sectors. The new data protection requirements impose transaction costs, thereby discouraging firms from collecting and sharing data with third parties. Businesses that depend on personal data to offer their services are possibly at a disadvantage. Studies particularly highlight the negative effects on small businesses.

Gal and Aviv(2020) use a legal perspective to analyze how GDPR influences the competitive dynamics of the data market. They highlight that the legal limitation on data collection and sharing changes market structures. First, the compliance requirements by all parties involved in data processing prevent companies from merging different databases, thereby limiting firms' ability to develop new(or improve existing) data-based products or services. Second, restrictions on sharing data may also prevent businesses from acquiring data necessary to improve operations, especially when data costs are high. Third, large firms' comparative advantage may increase market concentration as they are in a better position to collect and process data. Also, the limits on data can prevent companies from entering or operating in the EU market altogether.

The explicit user consent requirement is particularly burdensome for data-intensive businesses. Web technology companies that offer services related to tracking user behavior and online marketing now have more limited access to data. Campbell, et al.(2015) examine the effects of obtaining consent through the opt-in policy and find that it imposes additional costs on specialized, smaller firms. Consumers are likely to decline permission to use their data because privacy notices make them aware of data policies. In addition, data policy notifications can interrupt the online experience, leading consumers to leave the website. These findings are consistent with Aridor, et al.(2020) analysis of new opt-in consent requirement under GDPR.

Using a difference-in-differences method, they observe that the new consent condition has led to a 12.5 percent decline in the intermediary-observed consumers in the online travel industry, as measured by changes in web cookies.

Further, studies find that GDPR reduces incentives to share data. If user data are transferred externally, companies collecting data must ensure that businesses processing data are GDPR compliant. Violation of the law can result in a severe fine of up to 20 million euros or 4 percent of global revenue. Batikas, et al.(2020) find that several websites reduced third-party domains on their sites after GDPR implementation. Specifically, it led to a reduction of 12.8 percent in the use of third-party cookies on websites. As a result, the EU market of web technologies is now more concentrated, driven by an increase in Google's market share.

Forthcoming research reaffirms the market concentration of web technology vendors. Johnson and Shriver(2020) examine more than 27,000 global websites to analyze the changes in website use of online technology vendors. The findings show that GDPR resulted in a short-term decline of 15 percent in the website-vendor relationship. Importantly, the study suggests that market concentration increased by 17 percent, possibly because of the drop in small technology vendors.

Research on privacy regulation also suggests that strict requirements may benefit large online platforms such as Facebook and Google. Advanced use of technology allows large companies to collect, store, and use high-volume data directly. Because of multiple product offerings, large platforms can also effortlessly get user permission(Campbell, et al., 2015). The access to and the advantage of data aggregation facilitates large platforms to profile consumers for better advertising and development of new products(Condorelli & Padilla, 2020).

Lastly, Jia, et al.(2020) demonstrate that GDPR has reduced venture investments. They focus on understanding investors' preference to invest locally in the post-GDPR world. By comparing tech investments in EU by local and U.S. investors, they find that after the implementation of GDPR, the number of monthly EU foreign deals declined by 22.20 percent compared to 15.80 percent for domestic investments. Findings are also consistent with previous research by Jia, et al.(2018), in which they suggested a decrease in EU technology venture investments.

7. *Innovation*

Foster, et al.(2018) note that measuring innovation can be challenging and that "much of the focus in the literature [involves]…measuring inputs to innovation(such as R&D expenditures) or proxies for the output of innovation(such as patents)." However, they posit that due to the strong link between firm entry and exit and productivity, innovation can be indirectly measured by observing these effects in markets. In particular, they focus on innovation driven by surges in market entry by younger firms—particularly those in High Tech sectors—and find that surges are followed by increases in productivity growth(Foster, et al., 2018, 1, 4).

Notably absent from the literature are

systematic studies of firm entry and exit related to productivity, although Foster, et al.(2018) may very well provide an avenue for inquiry. For example, Hoofnagle, et al.(2019, 76-77) suggest that these dynamics are likely to manifest most clearly in data processing methods that are, by design, disfavored by GDPR—like third party processing(e.g., Big Data business models). Relatedly, in a recent survey of AI startups, James, et al.(2020) find that 65 percent of firms surveyed had less than 50 employees while many of these firms also had to reallocate their limited resources to comply with the new requirements of GDPR.

8. *Marketing Activities*

A study by Goldfarb and Tucker on the effect of the EU's 2002 ePrivacy Directive provided early empirical evidence that privacy regulation reduced the effectiveness of online advertising in an economically meaningful way(Goldfarb & Tucker, 2011, 57). They estimated an association between passage of the EU law and a reduction in advertising effectiveness of 65 percent. The implication of reduced effectiveness is that advertisers would have to spend almost thrice as much on advertising to achieve the same level of effectiveness—with particular implications for the monetization of "general content" providers including news websites(Goldfarb & Tucker, 2011). A study by Goldberg, Johnson, and Shriver(2019) analyzed the data of over 1,500 firms' web traffic and estimated that page views and site visits fell by approximately 10 percent with an 8.3 percent reduction in revenues—which translates into an $8,000 reduction revenue every week for the median site in their sample.

9. *Cross-Border Data Flows*

GDPR mandates that data transfer outside the EU requires the receiving country to provide adequate protection. It implies that the country must have security standards to comply with the EU regulations. This requirement creates new challenges for other countries trading with the EU on services or products. Cross-border data flows are particularly required for certain business outcomes in the digital economy(OECD, 2018). It has allowed consumers to access goods and services from different countries. Small and Medium Enterprises benefit from technology services such as cloud computing, which might be hosted in other countries. In short, the online world has reduced transaction costs for individuals and businesses.

However, given the sensitive nature of personal data, governments prohibit or impose conditions on international transfers. GDPR introduces two conditions: first, the company handling data must be GDPR compliant. Second, the country where the data is transferred must have adequate safeguards for personal data. Activities covered under these requirements include the transfer of data to public entities for investigation, contracting/hiring external service providers, or other activities that may transfer EU residents' personal data to other countries.[9)]

9) https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en.

These requirements can lead to two primary outcomes. First, it could expand data protection policies in other countries. Second, it can reduce cross-border data flow/trade of goods or services. Since the introduction of GDPR in 2016, the privacy regulations in other countries are often inspired by GDPR principles or enforcement mechanisms(Greenleaf, 2019). Countries such as Thailand, Korea, India, and Indonesia offer similar protections as those provided by GDPR. Bendiek and Romer(2019) state that the extra-jurisdictional requirements of the legislation put pressure on global companies operating in the EU not only to implement the regulation but also to store their data in Europe.

Studies have also assessed the economic impact of restrictions on data flows. Bauer, et al.(2013) evaluated the economic impact of GDPR using a computable general equilibrium GTAP model. The results suggest that cross-border trade disruption reduces EU's GDP. Particularly, it noted that the negative impact of GDPR would be between -0.8 percent and -1.3 percent. Ferracane, Kren and Marel(2020) investigate how data policies influence the productivity of data-intense firms. The study finds that stricter regulations negatively affect a firm's economic performance in data-intensive sectors. It also highlights that the negative effect is more significant for domestic restrictions compared to cross-border rules.

Data localization is another aspect of GDPR. Chander and Le(2014) argue that localization rules benefit only a small number of domestic enterprises, but it has major consequences for the economy as it increases the costs to businesses, thereby reducing the incentives for data localization. Data centers are costly to build. In the U.S., a company has to spend $43 million and, in Brazil, around $60.9 million. They also limit innovation by restricting data flows for cloud computing and the Internet of Things. However, EU's emerging external trade policy can minimize the effects of its regulation(Yakolova & Irion, 2020).

On a positive note, GDPR does not affect the internet connection network. Zhou, et al.(2020) investigate the effect of GDPR on global internet interconnection. Utilizing interconnection agreements between networks, they compare the changes in the European Economic Area(EEA) and non-EEA OECD countries post-GDPR. Evidence reveals zero effects; the interconnection network in EEA increased at the same rate as networks in non-EEA OECD countries. Also, the interconnection between each pair of a network was not affected by GDPR.

Ⅲ. *Lessons for Policymakers*

As digital markets continue to innovate—in part fueled by leveraging the ubiquitous nature of personal data—governments must work to balance regulation of privacy and data protection against the benefits gained from continued innovations in emerging technologies. Heterogeneous preferences for privacy and data protection, divergent legal and regulatory foundations, and the uncertain direction in which new technologies will innovate make data governance all the more difficult. This is particularly true given the highly globalized

nature of this sector—where governments must also consider how to avoid creating unnecessary barriers to international data flows.

As a result, policymakers will have to decide which combination of approaches and regulatory instruments are most appropriate for data governance(Gunningham & Sinclair, 1998). For instance, McGeveran(2016) advances "responsive regulation" as a workable solution, pointing out that "regulators must leave companies enough room to experiment, and users enough time to adjust, or risk thwarting desirable improvements." Similarly, others have advanced iterative, flexible approaches to regulation including the use of "regulatory sandboxes" to facilitate the development of new business models while allowing governments time to learn about potential risks and harms that may be ameliorated by policy intervention(OECD, 2019). Finally, achieving regulatory harmonization may not always be a feasible(or even desired) outcome for many countries with regards to preserving the international flow of data. This suggests that policymakers may find the need to supplement regulatory cooperation(e.g., treaties, mutual recognition agreements) with informal "soft law" governance approaches that Marchant and Allenby(2017) suggest could include: "private standards, guidelines, codes of conduct, and forums for transnational dialogue."

The aforementioned makes it necessary for policymakers to engage with evidence of the link between data protection regimes that are currently being implemented—such as the EU's GDPR—and real-world market outcomes. To date, researchers have focused on GDPR's effect on data-intensive sectors. It is evident that web-based businesses have had to adjust their business models to comply with the new data protection rules. However, we know much less about the extent to which this applies to other sectors. Also, online platforms such as social media or search engines are dependent on personal data for revenues, which may not be the case for businesses with other approaches—even within the same sector.

Finally, data protection regulations must be understood in their country context. In Europe, the emphasis on the fundamental right to data protection and privacy shapes regulatory policy. Despite the associated costs, European policymakers found it necessary to implement GDPR to promote these political priorities(Hoofnagle, et al., 2019). In comparison, U.S. discussions about privacy regulation have focused on issues of innovation and the potentially disproportionate burden of compliance on small businesses. Importantly, unlike the EU, the U.S. does not approach data protection from a rights-based perspective. U.S. regulations often follow a cost-benefit analysis framework to inform the best policy option. Therefore, as countries think about data protection, they have to consider their regulatory perspective.

Ultimately, governments will not be designing regulation in a vacuum; data protection regimes like the EU's GDPR and emerging regimes like the U.S.'s CCPA are already being implemented—providing an opportunity for learning about the extent to which different approaches function in particular contexts. Given the large size of

the U.S. and EU data markets, it remains to be seen whether other jurisdictions adopt similar governance regimes or pursue alternate strategies for data governance.

Lastly, from the above discussion, we find it particularly timely for researchers and practitioners to inform the policy debate by generating such evidence(Cordes & Pérez, 2019). More evidence is needed on the link between regulation and market outcomes including: firm competitiveness and market concentration, innovation, and the effects of compliance burdens on small and medium-sized businesses versus large, industry incumbents like Facebook and Google. Additionally, the effect of data protections on other sectors can also help in understanding the link between policies and market outcomes. For example, the U.S. has sectoral restrictions in health and finance—how have these regulations affected innovation?

■ References

Acemoglu, D., Akcigit, U., Alp, H., Bloom, N. & Kerr, W. (2018). "Innovation, reallocation, and growth." *American Economic Review, 108*(11), 3450-91.

Aridor, G., Che, Y. & Salz, T. (2020). *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR* (No. w26900). National Bureau of Economic Research.

Ayres, I. & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press, USA.

Bendiek, A. & Römer, M. (2019). "Externalizing Europe: the global effects of European data protection." *Digital Policy, Regulation and Governance*.

James, E., Stephen, M., Lydia, R. & Robert, S. (2020). "GDPR and the Importance of Data to AI Startups." *Available at SSRN 3576714*.

Bradford, A. (2012). "The brussels effect." *Northwestern University Law Review, 107*(1), 1-68.

Campbell, J., Goldfarb, A. & Tucker, C. (2015). "Privacy regulation and market structure." *Journal of Economics & Management Strategy, 24*(1), 47-73.

Cave, J., Schindlet, H., Robinson, N., Horvath, V., Castle-Clarke, S., Roosendaal, A., Kotternik, B. & Marcus, S. (2012). *Data Protection Review: Impact on EU Innovation and Competitiveness*. Directorate-General For Internal Policies. European Parliament. http://www.europarl.europa.eu/studies

Chander, A. & Le, U. (2014). "Breaking the Web: data localization vs. the global internet." *Emory Law Journal, Forthcoming*.

Chander, A., Kaminski, M. & McGeveran, W. (2020). Catalyzing Privacy Law. *Minnesota Law Review. Forthcoming. Available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3433922.

Christensen, L., Colciago, A., Etro, F. & Rafert, G. (2013). The impact of the data protection regulation in the EU. *Intertic Policy Paper, Intertic*.

Ciriani, S. (2015). "The economic impact of the European reform of data protection." *Communications & Strategies,* (97), 41-58.

Condorelli, D. & Padilla, J. (2020). "Harnessing Platform Envelopment in the Digital World." *Journal of Competition Law & Economics, 16*(2), 143-187.

Cordes, J. & Pérez, D. (2019). "Measuring the Costs and Benefits of Privacy Controls: Conceptual Issues and Empirical Estimates." *Journal of Law, Economics & Policy, 15*(1), 1-18.

European Commission (2012). Impact Assessment: 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). *Commission Staff Working Paper*. European Commission. Brussels.

European Data Protection Supervisor (n.d). *International Transfers*. https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en.

Ferracane, M., Kren, J. & van der Marel, E. (2020). "Do data policy restrictions impact the productivity performance of firms and industries?" *Review of International Economics, 28*(3), 676-722.

Foster, L., Grim, C., Haltiwanger, J. & Wolf, Z. (2018). *Innovation, productivity dispersion, and productivity growth* (No. w24420). National Bureau of Economic Research.

GDPR (2016). Article 4: GDPR Definitions. General Data Protection Regulation. https://gdpr.eu/article-4-definitions/.

GDPR (2016). Article 4: GDPR Definitions. General Data Protection Regulation. https://gdpr.eu/data-protection-impact-assessment-template/.

Goldberg, S., Johnson, G. & Shriver, S. (2019). Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes. *Available at SSRN 3421731*.

Goldfarb, A. & Tucker, C. (2011). "Privacy regulation and online advertising." *Management science, 57*(1), 57-71.

Gunningham, N. & Sinclair, D. (1998). Designing smart regulation. In *Economic Aspects of Environmental Compliance Assurance. OECD Global Forum on Sustainable Development.*

Haltiwanger, J., Jarmin, R., Kulick, R. & Miranda, J. (2017). High growth young firms: contribution to job, output, and productivity growth. In *Measuring entrepreneurial businesses: current knowledge and challenges* (pp. 11-62). University of Chicago Press.

Hoofnagle, C., van der Sloot, B. & Borgesius, F. (2019). "The European Union general data protection regulation: what it is and what it means." *Information & Communications Technology Law, 28*(1), 65-98.

Hoofnagle, C., van der Sloot, B. & Borgesius, F. (2019). "The European Union general data protection regulation: what it is and what it means." *Information & Communications Technology Law, 28*(1), 65-98.

IAPP (2018). IAPP-EY *Annual Governance Report 2018*. https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/.

Jia, J., Jin, G. & Wagman, L. (2018). *The short-run effects of gdpr on technology venture investment* (No. w25248). National Bureau of Economic Research.

Jia, J., Jin, G. & Wagman, L. (2020). GDPR and the Localness of Venture Investment. *Available at SSRN 3436535*.

Johnson, G., Shriver, S. & Goldberg, S. (2020). Privacy & market concentration: Intended & unintended consequences of the GDPR. *Available at SSRN 3477686.*

Jones, M. & Kaminski, M. (2020). "An American's Guide to the GDPR." *Denver Law Review, 98*(1).

Li, H., Yu, L. & He, W. (2019). "The impact of GDPR on global technology development." *Journal of Global Information Technology Management, 22*(1), 1-6.

Marchant, G. & Allenby, B. (2017). "Soft law: New tools for governing emerging technologies." *Bulletin of the Atomic Scientists, 73*(2), 108-114.

McGeveran, W. (2016). "Friending the privacy regulators." *Arizona Law Review, 58*(4), 959-1026.

Nikolaos, T. (2018) The 2018 Buzzword: "GDPR," and How It practically Affects Corporations in the EU and the US, TTLF Working Papers No. 32, Stanford-Vienna Transatlantic Technology Law Forum.

Organization for Economic Co-operation and Development (2018). Trade and Cross-Border Data Flows. Working Party of Trade Committee. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/

FINAL&docLanguage=En.
Organization for Economic Co-operation and Development (2019). Going Digital: Shaping Policies, Improving Lives. OECD Publishing, Paris. https://doi.org/10.1787/9789264312012-en.
Spiekermann, S., Acquisti, A., Böhme, R. & Hui, K. (2015). "The challenges of personal data markets and privacy." *Electronic markets, 25*(2), 161-167.
Thirani, V. & Gupta, A (2017). The Value of Data. *Industry Agenda*. World Economic Forum. https://www.weforum.org/agenda/2017/09/the-value-of-data/
Yakovleva, S. & Irion, K. (2020). "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade." *International Data Privacy Law*.
Zarsky, T. (2017). "Incompatible: the GDPR in the age of big data." *Seton Hall Law Review, 47*(4), 995.
Zhuo, R., Huffaker, B. & Greenstein, S. (2019). *The Impact of the General Data Protection Regulation on Internet Interconnection* (No. w26481). National Bureau of Economic Research.