Regulatory Studies Center
THE GEORGE WASHINGTON UNIVERSITY

Improving regulatory policy through research, education, & outreach

Two Years Later: A Look at the Unintended Consequences of GDPR

By: Aryamala Prasad | September 2, 2020

In brief…

Two years after implementing GDPR, the EU confirmed it achieved the intended outcome of strengthening individual rights. But the regulation has created new challenges by disproportionately benefiting Big Tech as a result of smaller firms' inability to bear the regulatory costs.

In May 2018, the European Union (EU) implemented the General Data Protection Regulation (GDPR) to safeguard personal data. Two years later, the EU confirmed the regulation achieved the intended outcome of strengthening individual rights. But the regulation has created new challenges by disproportionately benefiting Big Tech as a result of smaller firms' inability to bear the costs related to myriad requirements. Recent studies explore the reasons for this troubling and unintended consequence of GDPR on competition and market concentration.

High Compliance Costs

At the outset, high compliance costs largely affect small and medium businesses. GDPR imposes strict obligations regarding the collection, processing, storage, and use of data. Companies need to ask for explicit consent to collect and process personal information. They must inform consumers about what data are being collected and if/how those data are shared with third parties. Additionally, data protection requirements extend beyond initial transactions between businesses and consumers; and businesses that collect and process data need to incur the costs of being able to fulfill requests including data access, correction, and erasure. Companies also cannot store data longer than necessary. Finally, because of its extraterritorial scope, GDPR applies to any business that collects data from EU residents, regardless of location.

International Association of Privacy Professionals estimated that medium-sized companies spent close to $3 million in 2017-2018 to fulfill the regulatory requirements, and an average U.S. Fortune 500 firm paid $16 million. Regulatory costs forced several newspapers and advertising firms to exit the EU market, and many small European firms are struggling to comply with the requirements.

Obtaining Informed Consent

The new opt-in consent requirement reduces data availability. Without explicit consent, firms cannot track consumers across websites or share data with third parties. Research shows requiring explicit opt-out consent deters more consumers from using the website by familiarizing them with data policies or interrupting the online experience. Further, the transaction costs associated with obtaining consent negatively affect smaller firms. As a result, firms collect far less data for targeted services and advertising. Post-GDPR, a third-party data intermediary experienced a 12.5 percent drop in user data for the online travel industry.

On the other hand, large platforms are able to gather more data by leveraging multiple product offerings. GDPR does not restrict internal data sharing after obtaining initial user consent. Google has immensely benefited from this provision; in 2012, Google created a broad privacy policy by consolidating 60 privacy notices. Hence, it can effortlessly merge data across services to create a comprehensive database. In contrast, external data sharing requires additional informed consent, and mandates data suppliers to monitor and ensure that the data are processed as per the user consent. Internal data transfers have helped Google and Facebook to strengthen their market position by collecting reams of data for targeted advertising.

However, large online platforms may be in violation of the *purpose limitation* principle. The law restricts businesses from processing data more than required for the initial purpose. In 2018, Germany's Federal Cartel Office (FCO), under its competition law, prohibited Facebook from combining data from multiple services. It determined that Facebook was exploiting its dominant market position to insist on conditional user contracts. When Germans agree to share their data with Facebook.com, they also have to permit data processing by other Facebook-related services. FCO observed that Facebook data handling practices are in violation of GDPR as there is no justification for collecting or processing data from multiple services to fulfill its contractual obligation related to Facebook.com services. On Facebook's appeal, a Higher Regional Court in Düsseldorf suspended the order last year. But recently the German Federal Court of Justice upheld the FCO findings on Facebook's practices.

Data Sharing Limitations

Additionally, data sharing limitations also disadvantage smaller firms. Businesses are now liable for privacy violations by third parties. If user data are shared externally, companies collecting data must ensure GDPR compliance. Failure to conform can result in a severe fine of up to 20 million euros or 4 percent of global revenue. The high cost of violations dictates a more cautious approach. Websites reduced the use of third-party technologies such as cookies by 12.8 percent in the EU. Also, businesses prefer to contract with large web-technology providers as they are better positioned to fulfill the legal requirement. A study found that a week after GDPR implementation market concentration increased by 17 percent because websites dropped smaller vendors.

Additionally, large companies such as Google limit access to their data. After GDPR implementation, Google restricted transfer of advertising data available through DoubleClick ID, a tool that allows marketers to measure and compare audience reach. Earlier, when Google removed third-party advertising on YouTube, its competitor AppNexus lost access to important data, and customers eventually moved to Google. Smaller web technology vendors face more challenges because of their dependence on data from multiple sources.

Venture Investments

Perceived risks and uncertainty also decreased investments in new ventures. Between May 2018 and April 2019, EU firms experienced a 26.1 percent decrease in monthly venture deals. The average amount of money companies raised fell by 33.8 percent. The decline was higher among foreign investors. However, domestic investments continued at the same rate; possibly because of the information investors have about local enforcement or their ability to handle risks due to local presence. Nevertheless, strict privacy regulation can lead to reduction in foreign investments.

Conclusion

When GDPR was implemented, the European policymakers emphasized the individual right to data protection. The EU's recently released report highlights the effectiveness of GDPR by citing the increased awareness of data protection among individuals. According to the Eurobarometer survey, 51 percent are aware of the right to access their personal data held by private companies. And data protection authorities reported around 275,000 complaints between May 2018 and November 2019.

While the regulation has empowered citizens, it has also negatively affected small businesses and increased market concentration. The European experience particularly highlights the challenges associated with data sharing in the digital sector. It appears that the European Commission is aware of the potential difficulties in development of new technologies and exploring ways to reduce barriers to innovation. However, it remains to be seen how the EU will respond to these challenges.