

CYBER STRATEGY & POLICY: POLICY ANALYSIS PAPER 4

Ean N. Miller

Old Dominion University

CYSE 425W: Cyber Strategy & Policy

Professor Teresa Duvall

November 17, 2024

The General Data Protection Regulation, enacted in 2018 by the European Union, is the standard against which global conversations about privacy and data protection are based. It was made to empower people with more control over their personal information, thus setting the base for almost all privacy regulations worldwide. Actionable application outside of Europe applies to any organization that deals in processing the personal data of citizens of the EU. It was created due to concerns about the rise in data breaches, personal data misuse, and increased technological company powers. The regulation aims to give a clear path on the collection, storage, and use of data, while there are severe penalties for those who do not comply, as Teixeira et al. (2020) reported. The societal impact of the GDPR is profound, influencing not only corporate practices but also how individuals view and protect their data. It reflects a shift towards a more rights-based approach to data protection, responding to widespread public outcry about privacy violations (Fan, 2021). The global reverberations of the GDPR highlight its cultural importance, sparking similar data protection initiatives in other countries and regions (Newman & Jang, 2020). These changes mark the importance of regulation in shaping contemporary data protection laws and broader societal attitudes toward digital privacy and corporate responsibility.

The General Data Protection Regulation (GDPR) was created in response to growing concerns over privacy erosion in the digital age. As the internet expanded, companies began collecting and monetizing personal data without individuals' consent, turning it into a valuable commodity. Incidents like the Cambridge Analytica scandal, where millions of Facebook users'

data were misused for political purposes, highlighted the risks of unregulated data exploitation, sparking public demand for stronger regulations (Fan, 2021).

The GDPR addressed this imbalance by imposing transparency and accountability on data controllers. It empowers individuals by granting them the right to access, correct, and delete their data, giving them greater control over their personal information (Newman & Jang, 2020). The regulation reflects a cultural shift in Europe, where privacy is viewed as a fundamental human right, contrasting with regions like the U.S., where data protection is often seen as a consumer choice. This shift underscores the growing global consensus that privacy should be a standard right, not a privilege (Teixeira et al., 2020).

Thus, the GDPR is not only a legal response to changed technological developments but also one that realizes that personal data needs protection in a world increasingly exploiting it for commercial and political gains.

The GDPR has reshaped interactions between individuals, corporations, and governments. For individuals, it has heightened awareness of personal data rights, encouraging vigilance over privacy. Organizations face substantial fines for non-compliance, compelling them to prioritize privacy in their operations. However, small businesses and marginalized groups often struggle with compliance, as the GDPR's complexity and enforcement mechanisms can disproportionately burden them. Critics argue that such groups risk being sidelined, deepening existing inequalities in the digital economy.

The GDPR, in addition, has influenced global data protection norms. Other countries, such as Brazil and Japan, have implemented similar legislation, highlighting how the GDPR aids

in cultivating a culture of accountability in privacy matters globally. Its extraterritorial reach encourages debates on sovereignty regarding when international organizations also have to apply the standards of the EU, which may be at variance with local regulations.

Cultural values promoting individual rights played a significant role in shaping the GDPR. The European focus on human dignity and privacy as fundamental human rights contrasts with regions like the United States, where corporate innovation and free-market principles often take precedence. This cultural divergence explains varying global responses to privacy regulation.

Subcultural empowerment through the GDPR has allowed advocacy groups to act as watchdogs. NGOs utilize Article 80 and other provisions allowing third-party complaints to advocate accountability. This grassroots method of enforcement demonstrates a sense of activist civil society's role in the functional application of the GDPR, creating almost a participatory governance model.

The GDPR is a milestone of digital governance that bridges the gap between society's demands for privacy through regulation. Its strengths lie in increasing awareness and a globally induced trend of accountability, yet it remains problematic, especially for impoverished, socially marginalized, and small businesses. Cultural resonance and changing applications show the deep impact of the GDPR on the social fabric in the Digital Age.

References

- Fan, M. (2021). *The hidden harms of expanding privacy penalties*. CLTC Berkeley. Retrieved from
<https://cltc.berkeley.edu/2021/08/20/the-hidden-harms-of-expanding-privacy-penalties/>
- Newman, A., & Jang, W. (2020). *Enforcing European privacy regulations from below*. CLTC Berkeley. Retrieved from
<https://cltc.berkeley.edu/2021/08/20/enforcing-european-privacy-regulations/>
- Teixeira, R., et al. (2020). *The right to data access*. Oxford Academic. Retrieved from
<https://academic.oup.com/spp/article/47/5/616/5780440>