

The EU's Novel Data Regulation: Changing the Face of the Internet

No. 54 May 2018

By Michael Amoah Awuah

Have you recently realised that your most reliable social media platforms and online retailers have sent you notifications on updates to their terms on personal data settings? This is not coincidental; the EU is getting tougher on internet privacy. Coming into effect on 25 May 2018 is the EU's novel set of privacy rules, which has been dubbed by technology experts and public policy analysts as arguably changing the face of the internet for everyone.^{1,2} The EU's new privacy rules—the General Data Protection Regulation (GDPR)³—are poised to sanitise the grey and muddled areas of internet privacy issues. The General Data Protection Regulation will be directly applicable in all member states and is to harmonise data privacy laws across Europe—and probably beyond. Herewith, the EU enforces the right of personal data protection.

So, what is the GDPR?

1. The GDPR (Regulation (EU) 2016/679) was passed by the European Parliament in 2016 and is set to take effect in 2018. It substitutes the 1995 EU Data Protection Directive, and in its new form of being a regulation, also supersedes national law.

2. The GDPR standardises data protection laws across all 28 EU member states and enforces strict new rules on how companies and governments alike manage, control, process, and share personally identifiable information (PII). It extends the protection of personal data and data protection rights by giving enforceable rights to

natural persons in the EU.

3. The GDPR mandates companies to comply with requirements to give internet users “clear and transparent notice”⁴ on how their data will be used.

4. The GDPR is applicable to all organisations holding and processing personal data in the EU, irrespective of the geographic location of the legal entity of the organisation. If an organisation offers goods or services to, or monitors the behaviour of EU residents, it must meet GDPR compliance requirements. Moreover, the GDPR applies to organisations outside of the EU regardless of their awareness of the law. Non-compliance penalties are set high enough for the industry to pay attention. Fines for serious violations can be as high as 20 million euros or 4 per cent of a company's total global revenue, whichever is larger.

5. Numerous essential items are contained in the regulation, including increased fines, breach notifications, opt-in consent, and responsibility for data transfer outside the EU. Consequently, the impact to businesses is huge and will permanently change the way in which customer data is collected, stored, and used.

In excess of 100 states and independent jurisdictions around the globe have now accepted comprehensive data protection and privacy laws to protect personal data held by private and public bodies.⁵ In addition, 40 countries and jurisdictions have pending bills or initiatives.

The perceived effect of the GDPR is that it raises the bar immensely, making it the gold standard for obtaining personal data—unlike which has ever been seen before. By default, any time a company collects personal data on an EU resident, it will need explicit and informed consent from that person. And again, it provides this individual the right to seek explanation on the content of a particular algorithm in relation to his or her personal data.⁶ Even though this has been seen to be the status quo, the alleged violations of Cambridge Analytica – Global Science Research and the Facebook data breach,⁷ make the roll-out of this potent EU regulation all the more imminent.

Through the GDPR the EU's normative and regulatory might is again revealed. The far-reaching arm of this new legislation has triggered most companies—even those outside of the EU, especially in the US—to aim towards a single set of privacy rules. However, some analysts have observed that this could lead to the dividing of the internet space between EU data preferences and the rest of the world. Whichever side of the divide one may find themselves on, a radical change in how the internet is governed with respect to user data and its accompanying data issues will be visible.

Lastly, with the implementation of the GDPR, the EU has paved a way for a possible systematic regulation of the internet. Especially since the advent of information and communication technologies, sector-specific regulation has been the EU's mainstay, and will increase in importance for ICT with the further development of the Digital Single Market. Varied attempted approaches to regulate the internet have sought to adapt the vestiges of previous processes, such as net neutrality and common carrier rules.⁸ At this juncture in the history of the internet, due to better data protection as well as

the free movement of such data, the EU is in better stead to provide best practice in the regulation of social media platforms—and by extension the entire gamut of internet services. This attempt for the systematic regulatory governance of the internet—inherent in the GDPR—would curb what critics have called the zombie-like nature⁹ of previous data protection laws, could fully unleash the trend-setting and real possibility of effective personal data protection, and would establish internet governance unseen elsewhere in the world.

The ultimate aim of the European Union's General Data Protection Regulation seeks to essentially "strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the digital single market" but its impact is changing the face of the internet as we know it.

Michael Amoah Awuah is a Research Fellow at the Center for European Integration Studies (ZEI) and currently working on his doctoral project "Rationale for Energy Governance in West Africa: Potential and Obstacles".

Endnotes:

1. Brandom, Russell. *How Europe's new privacy rule is reshaping the internet.* (2018).
2. Albrecht, Jan Philipp. *How the GDPR Will Change the World.* *European Data Protection Law Review* 2, 287–289 (2016).
3. Regulation (EU) 2016/ 679 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.
4. European Commission. *Data protection in the EU.* European Commission - European Commission.
5. Banisar, David. *National Comprehensive Data Protection/ Privacy Laws and Bills 2018.*
6. Goodman, Bryce. & Flaxman, Seth. *European Union regulations on algorithmic decision-making and a 'right to explanation'.* *arXiv:1606.08813 [cs, stat]* (2016).
7. Madrigal, Alexis. C. *What Took Facebook So Long? The Atlantic* (2018).
8. Ehrlich, Ev. *A Brief History of Internet Regulation.* *Progressive Policy Institute* 20 (2014).
9. Koops, Bert.-Jaap. *The trouble with European data protection law.* *International Data Privacy Law* 4, 250–261 (2014).

ZEI Insights are part of the Research Project - Governance and Regulation in the EU: [The Future of Europe](#)

ZEI Insights provide commentary and critical analysis on governance and regulation issues related to the future of the European Union. Authors are responsible for their own views.