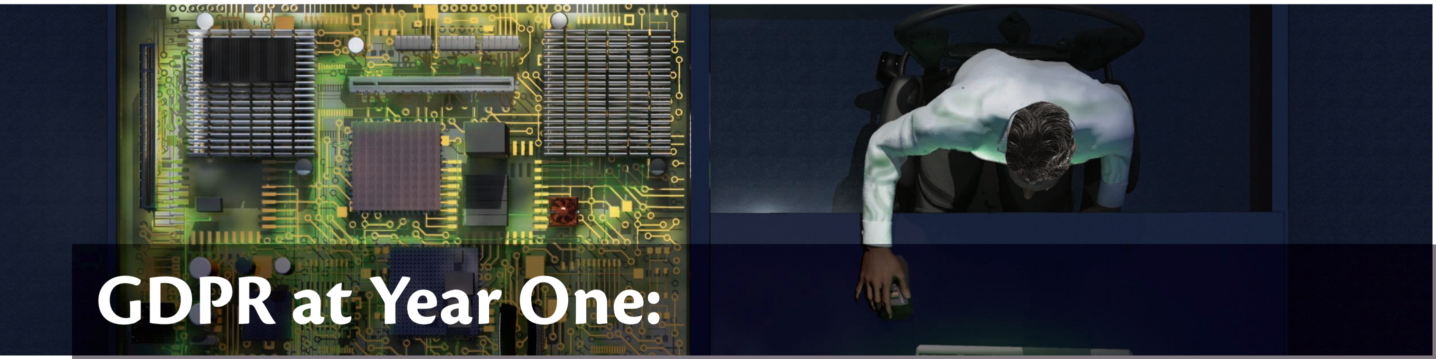

GDPR at Year One: Enter the Designers and Engineers

Omer Tene | International Association of Privacy Professionals
Katrine Evans | Hayman Lawyers
Bruno Gencarelli | European Commission
Gabe Maldoff | Covington & Burling LLP
Gabriela Zanfir-Fortuna | Future of Privacy Forum

Nearly a decade in the making, the General Data Protection Regulation (GDPR), Europe's massive overhaul of its privacy and data protection laws, came into effect to great fanfare in May 2018. Impacting every area of an economy marked by technological and data innovation, including the public and private sectors, finance and health care, retail and education, transportation, pharmaceuticals, utilities, and scientific research, the GDPR carried immense promise but also many implementation challenges and interpretation complexities. A year in, it is not too soon to pause for reflection and to explore the reform's effect on corporate and organizational data practices, particularly at the intersection of policy, law, and engineering.

The GDPR is grounded on a rich policy foundation. For the most part, its principles are not new. Many of the law's provisions are a direct continuation of the European data protection regime set forth in the 1995 Data Protection Directive (DPD). The DPD, in turn, came to harmonize then-existing European Member State data protection legislation, some of which dated to the 1970s and 1980s. France, for instance, passed its data protection law in 1978; Sweden legislated its Data Act in 1973.

Privacy and data protection laws proliferated not just in Europe. In 1959, the New York City Bar Association formed a special committee to study the effects of science on the law. The Committee's 1966 report, largely authored by Columbia University scholar Alan Westin, laid the foundation for the first-ever articulation of the fair information practice principles (FIPPs). The FIPPs were further developed in Westin's seminal work, *Privacy and Freedom*, as well as in a committee report to the U.S. Department of Health, Education, and Welfare that he authored in 1973. Like the GDPR, the DPD and earlier data protection initiatives were portrayed, at the time, as foolhardy attempts to regulate a matter—data—that was as ephemeral as the air we breathe.

But the GDPR did innovate on several fronts, first and foremost in its recognition that to be effective data protection must descend from the ivory tower of jurists and academics, who can for years debate subtle nuances between the French and English wording of a recital, to the humdrum of ubiquitous organizational data flows on the ground. With implications in nearly every business workflow—including, for large companies, hundreds or thousands of IT systems and relationships with vendors, service providers, and customers located across the globe and communicating nonstop—data protection must

Digital Object Identifier 10.1109/MSEC.2019.2938196
Date of current version: 29 October 2019

transition from policymakers and lawyers to designers and engineers.

That need is reflected in the GDPR's turn toward privacy and data protection engineering. The definition of the term is evolving. The U.S. National Institute of Standards and Technology defines privacy engineering as "a specialty discipline of systems engineering focused on removing conditions that can create problems for people when system operations process their information."[1] That definition is broad enough to include process engineering as well as the engineering of products and services to mitigate privacy risks. The GDPR recognizes and sets forth detailed demands for both.

The GDPR embraces privacy process engineering in a set of accountability requirements. Accountability is one of the fundamental data protection principles, making organizations responsible for complying and demonstrating their compliance with the law. To do so, organizations must put in place appropriate technical and organizational measures, including adopting and implementing data protection policies; mapping and itemizing data flows; maintaining documentation of data processing activities; implementing appropriate security measures; recording and, where necessary, reporting personal-data breaches; carrying out and documenting data protection impact assessments; appointing a data protection officer; overseeing relations and contracts with vendors and service providers; managing user consent and cookie interfaces; rationalizing data storage and retention; and more. Accountability obligations are ongoing, meaning that organizations must continually review, audit, update, and amend the measures they put in place.

Accountability requirements have a rich data protection pedigree. Forty years ago, the Organization for Economic Cooperation and Development adopted accountability as one of the FIPPs in its 1980 "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." But only in the past few years have organizations begun to bridge the gap between the other FIPPs (such as data quality, openness, and purpose specification) and their accountability obligations, a divide that Deirdre Mulligan and Ken Bamberger characterized as "privacy in the books and privacy on the ground."[2]

To satisfy those requirements organizations need systems and technologies for managing data at scale. When it went into force, the GDPR stimulated a new industry sector that provides technological solutions for data governance and privacy program management. The International Association of Privacy Professionals' "Privacy Tech Vendor Report," which tracks the emerging sector, listed 50 companies when it launched in 2017 and now includes more than 200 vendors that provide technological compliance solutions. As organizations race to build their own internal capabilities for innovating privacy, external solutions are just the most visible sign.

The GDPR has catalyzed organizations to deploy privacy engineering in the design of new products and services. Article 25 expressly calls on organizations to implement data protection by design and by default. According to the U.K. Information Commissioner, "this means you have to integrate or 'bake in' data protection into your processing activities and business practices."[3] Under Recital 78 of the GDPR, such measures include data minimization, pseudonymization, and putting individuals in charge of their data.

More subtly, a general principle that data processing must be "fair," coupled with specific provisions that guide the meaning of free and informed consent, has brought design, user experience, and engineering to the heart of the privacy debate. It is no coincidence that the most significant enforcement action of the GDPR's first year—a €50 million fine, in France, against Google for allegedly coercing consent and not providing users with a clear notice or choice—took particular aim at the way information and choices were presented, not the content of the notices or the substance of the choices. Despite the density of its legal text, make no mistake, the GDPR is moving privacy from the province of lawyers to the realm of engineers, designers, data scientists, and IT professionals who are poised to shape the way we experience the services that rely on our data.

Increasingly, companies are adopting privacy and data protection as a competitive differentiator. Apple, the world's most valuable company, has made encryption, on-device data analysis, and tracking protection hallmarks of its products. In fact, in 2019 the company launched a marketing campaign for the iPhone, its premier product, under a privacy tagline. Together with other technology leaders, such as Google and Microsoft, Apple has also adopted differential privacy in certain circumstances to provide a baseline for the protection of users' data. A formal mathematical framework for quantifying and managing privacy risks, differential privacy provides provable protections against a wide range of attacks, in contrast to heuristic-based protections that may not withstand the test of time. Scientists are working to adapt other methodologies, such as secure multiparty computation and fully homomorphic encryption, to advance privacy goals.

When engineering for data protection and privacy, organizations often walk a fine line between, on the one hand, sacrificing data benefits—in fields ranging from economic efficiency to national security and public health—and, on the other hand, compromising individuals' fundamental rights. That balance, which is integral to the text of many GDPR provisions, such as the "legitimate interests of the controller" clause and the derogations for "scientific or historical research purposes," requires an attention to nuance that is often missing from public discourse and cannot be captured without a deep understanding of technology and the technical aspects of a service.

Consider facial recognition. It is one of the most hotly debated technologies, which has spawned outright bans in several U.S. localities and calls for specific regulation in the European Union. But facial recognition is not monolithic. It has many different use cases with widely varying data protection risks. Facial detection is unlike facial characterization, which differs from facial verification and facial identification. The policy implications are profound. With facial detection, a system distinguishes the presence of a human face or facial characteristics without creating or deriving a biometric template. With facial characterization, a system derives an individual's demographic information or emotional state without creating a unique biometric identifier that could be tracked over time. Facial verification (or authentication) confirms an individual's claimed identity by comparing a template generated from a submitted facial image with a specific known template generated from a previously enrolled image. Such one-to-one verification raises fewer data protection risks than facial identification, or one-to-many matching, whereby a system searches a database for a reference matching a submitted facial template and returns a corresponding identity.

Clearly, calls for banning facial recognition are too blunt. Do privacy advocates and legislative proponents of such a ban really mean to preclude camera makers from integrating autofocus features into new lenses (facial detection)? Or to prevent individuals from using facial scans to unlock their phones, ATMs, and medicine disbursements (facial verification)?

Those questions and the many others affecting every facet of digital technology raise a myriad of legal, ethical, and technical challenges that policymakers, regulators, and courts will have to unpack during the next few years. But, gone are the days when the engineers and technicians could sit on the sidelines. The meaning of the numerous implementations of the GDPR will not be decided only in the courtrooms and academic tomes but in the science of possibility and the design of the mundane.

New technologies will continue to promise unforeseen gains as they unearth novel privacy perils, and new legislation will continue to reach further into the process of technological development. Organizations will continue to deploy designers and engineers to create compliance processes, products, and services that seek to maximize data benefits while minimizing privacy and data protection costs. With any luck, designers and engineers will be there to ensure that we get the balance right. ■

References

1. National Institute of Standards and Technology, "What is privacy engineering?" Gaithersburg, MD. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/about
2. K. A. Bamberger and D. K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. Cambridge, MA: MIT Press, 2015.
3. Information Commissioner's Office, "Data protection by design and default," Wilmslow, U.K. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Omer Tene is with the International Association of Privacy Professionals, Portsmouth, New Hampshire. Contact him at otene@iapp.org.

Katrine Evans is with Hayman Lawyers, Wellington, New Zealand. Contact her at k.evans@haymanlawyers.co.nz.

Bruno Gencarelli is with the European Commission, Brussels, Belgium. Contact him at bruno.gencarelli@ec.europa.eu.

Gabe Maldoff is with Covington & Burling LLP, Washington, D.C. Contact him at gmaldoff@cov.com.

Gabriela Zanfir-Fortuna is with the Future of Privacy Forum, Washington, D.C. Contact her at gzanfir-fortuna@fpf.org.