

LEGAL AND PRIVACY

## Year of GDPR: Looking back and to the future

May 29, 2019



*Michael J. Becker is managing partner of Identity Praxis*

By **Michael Becker**

Subscribe to **Luxury Daily**  
Plus: Just released  
State of Luxury 2019 **Save \$246 ▶**

A year ago Saturday, May 25, marks the one-year anniversary of the GDPR (**General Data Protection Regulation**), a tsunami that washed onto the world's shores.

Even though the **GDPR** waters have yet to settle, it is abundantly clear that the world's topography has forever changed.

GDPR has triggered change across all five foundational pillars legal, economic, technology, social and political of the world's economies.

In the wake of GDPR, regions such as the European Union and Latin America, countries, states and companies around the world are responding to the call to give individuals self-sovereignty and authority over their identity and personal data.

To comply with these regulations, organizations must develop new processes, change their technology stacks, and appoint a chief data officer (DPO).

GDPR applies to any company with operations in the E.U. or to those that process personal data of European citizens or monitor the behavior of European citizens.

What are people's rights?

Under GDPR and similar regulations, people have rights to their personal information.

At a high-level, when referring to "people's rights," what this means is this that people have will have a right to:

- be informed on how their data is to be used by an organization and its partners
- access the data an organization and its partners holds on them
- rectification: the ability to correct the data an organization and its partners holds on them

- erasure, aka right to be forgotten: the ability to demand an organization and its partners delete the data they hold on them
- restrict processing: restrict and suppress how an organization and its partners use their data
- data portability: have the ability to ask for and receive a digital record of the data an organization holds on them
- object: the ability to object to the processing of their data in certain circumstance, e.g. scoring and profiling and automated marketing
- challenge automated decision making and profiling, meaning an individual can challenge an organizational decision if the decision was derived solely through an automated process
- equal service, not be discriminated against, even if they exercise their rights

Each and every one of the above rights is directional. Each right is independent and interdependent. They are, in most instances, not absolute, as they may only apply in certain circumstances.

GDPR-like regulations around the world

The waves generated by GDPR are reverberating around the world.

In Latin America, Argentina and Chile are looking to amend their existing laws (see [Law No. 25,326](#), and [Law No. 19,628](#) respectively).

Brazil is putting in place a new law (see [House Bill No. 53, of 2018](#)).

Mexico, Colombia and Peru are also working toward amending existing laws and adding new laws similar to GDPR.

India and Australia are recognizing the "human-right" to privacy, and South Africa is enacting the [Protection of Personal Information Act \(POPIA\)](#).

In the United States, California enacted the [California Consumer Privacy Act of 2018 \(CCPA\)](#) (California Consumer Privacy Act.) on June 28, 2018. Formally referred to as CA AB-375, CCPA will take effect on Jan. 1, 2020. Interestingly, the CCPA, in section 1798.125 (a) (1), recognizes the economic value of personal information, noting that "A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information."

Washington State ([Senate Bill SB 5376 2019-20](#)) and Commonwealth of Massachusetts initiated laws similar to GDPR to give individuals new rights and authority over their personal information.

Washington State's efforts appear to have stalled, but the Massachusetts law is still taking shape and is expected to take effect in 2023 ("An Act relative", 2019; Ropek, 2019).

Furthermore, individual U.S. cities and sectoral legislation are being enhanced and established to protect individuals' data and privacy.

For example, San Francisco this month banned government use of facial recognition (Van Sant & Gonzales, 2019). Washington, Texas and Illinois have similar provisions.

In addition, specific sectoral legislation such as the [HIPPA](#) rules around healthcare and [COPPA](#) rules around engaging children are being re-worked.

These are just a few of the regulatory changes occurring throughout the world.

Study and understand the regulations

It is important to study the details of every regulation to understand who they apply to, how they apply, the requirements that must be met to adhere to them, and the timings that must be recognized when an individual files a complaint.

For example, the thresholds to determine if a company must adhere to a regulation vary.

The GDPR applies to any company with operations in the E.U. or to those processing personal data of European citizens or those that monitor the behavior of European citizens.

For the CCPA to apply to an organization, the entity must have gross revenues in excess of \$25 million, or be in the business of buying, selling or processing the personal information of more than 50,000 data subjects (aka

individuals), households or devices, or derive 50 percent or more of its revenue from the sales for personal data.

As for how much time an organization has to comply when an individual enacts their rights, verbally or in writing, the timing may vary from a matter of days, months, or a year. The requirements may be different for each right and each regulation.

GDPR and the new regulations have teeth

One detail to pay special attention to when evaluating a regulation is that a regulation today may carry with it substantial fines.

GDPR, like its cousins, not only brings new rights to individuals and new requirements to businesses and technical processes that organizations must recognize and adhere to, it also brings quite a sizable fine if its requirements are not met.

In the case of GDPR, companies face fines of 4 percent of global revenues, or 20 million, whichever is larger.

Under the CCPA the fines are capped at \$7,500 per violation and \$2,500 per violation when nefarious intent is not present.

The IAPP (n.d.) "[GDPR One Year Anniversary Infographic](#)," as of May 25, 2018, shows that, since GDPR took effect last year, 500,000 DPOs have been registered (registering a DPO is a requirement of GDPR), a total of 89,000 data breach notifications have been filed (filing data breaches is another requirement of GDPR), nearly 280,000 consumer complaints have been registered, and there have been more than 56,000,000 in fines levied (which were mostly attributed to Google in France).

Be sure to revisit the IAPP's GDPR infographic, as they update it regularly.

Organizational response to GDPR

Industry titans have also started responding to society's demands for improved stewardship over personal data.

- Facebook CEO Mark Zuckerberg is repositioning Facebook by publicly announcing that "The future is private." Also, Facebook is introducing new privacy-centric capabilities (Statt, 2019).
- Google's CEO Sundar Pichai recently said that "privacy should not be a luxury good," but rather an inherent part of every product and service (2019).
- Apple CEO Tim Cook suggests that we are faced with a privacy crisis, that people are not the product (Eadicicco, 2019).
- Microsoft CEO Satya Nadella, speaking at the World Economic Forum in Davos, Switzerland, said that "privacy is a human right" (Nadella & Schwab, 2019).

Thinking beyond the legal checkbox to personal data exchange

Prosperity is on the horizon.

According to the United Kingdom government, in a 2018 report authored by Ctrl-Shift (2018), the impact and productivity to be had from empowering people with control over their personal data, not including growth from innovation, could generate as much as \$27.8 billion to the country's GDP.

Looking at country-level GDP is not the only metric to consider when thinking about the value that can be generated by giving people control of their data.

People can and will benefit directly from the exchange of their personal data, including the data generated from their labor or capital.

For example, Jaguar, in April 2019, [announced](#) that it is working on a program where people can sell the data collected by its connected car (Smith, 2019).

In this example, when the car detects a pothole it will collect the location of the pothole and sell this data to a local municipality.

Cryptocurrency payments for the data will be made directly to a person's Jaguar Smart Wallet. People can then use this income to pay for parking, tolls, charging stations and a cup of coffee.

ORGANIZATIONS BIG AND SMALL should not be resigned to simply comply with the rules laid down by the GDPR

Organizations and individuals should not be resigned to simply comply with the rules laid down by the GDPR and similar legislation. They should not be afraid to empower individuals and to give them control of their data.

Rather, to thrive in the wake of GDPR, companies should embrace change, adopt new systems, and overcome their challenges, and use this opportunity to re-configure their value chains, organizational systems, and business models, to innovate and, most importantly, to refresh and forge new bonds with the people they serve.

*NOTE: I am not a lawyer. Do not consider this article legal advice. Consult your legal counsel before executing plans to comply with GDPR or any regulation.*

*Michael J. Becker is managing partner of [Identity Praxis Inc.](#), San Mateo, CA. Reach him at [michael@identitypraxis.com](mailto:michael@identitypraxis.com).*

---

© 2020 Napean LLC. All rights reserved.

American Marketer is published each business day. Thank you for reading us. Your [feedback](#) is welcome.