Data Privacy: What 2019 Holds for U.S. Companies

January 23, 2019 Laura Prather, Andrew Van Osselaer

PRACTICES Intellectual Property

Introduction

The European Union's General Data Protection Regulation (GDPR) went into effect in May 2018,[1] clamping down on those that collect E.U. residents' personal data—wherever they may be.[2] There is much we could learn from the GDPR's growing pains; but the GDPR is still in its infancy, and legislative wheels are already turning at home: U.S. lawmakers have begun flirting with GDPR-inspired omnibus data-privacy regimes. As a result, companies do not have the luxury of adopting a wait-and-see approach to data privacy compliance. The time to get up to speed is now.

I. The GDPR Regime

The GDPR restricts "controllers" and "processors"[3] of E.U. residents' "personal data," which it defines as data "directly or indirectly" linked to an individual's identity or traits.[4] It serves three primary functions: it provides data subjects an array of substantive rights, it regulates controllers' and processors' conduct, and it sets penalties for violations.

A. Data Subjects' Rights

The GDPR creates several substantive rights, including the right not to have one's personal data processed without one's informed consent;[5] the right to know who has one's personal data, what that data is, and how it is being used;[6] the right to have one's data delivered in a portable format;[7] the right to revoke one's consent, have relevant data deleted (also known as the right to be forgotten), and have one's revocation communicated to subsequent data purchasers;[8] the right to correct errors;[9] the right to demand a human review of automated decisions based on one's personal data;[10] and the right not to be discriminated against for exercising one's rights.[11]

The GDPR forbids controllers and processors from charging fees for facilitating data subjects' rights.[12]

B. Rules for controllers and processors

The GDPR limits the transfer of GDPR-protected personal data to countries that do not offer adequate protection;[13] requires controllers and processors to notify their governing authority of personal-data breaches;[14] requires controllers and processors to implement "appropriate" data management and security measures,[15] and requires the heaviest users of personal data to keep records of their data processing activities and appoint data-protection officers.[16]

C. Enforcement and punishment

Unlike some U.S. regimes, the GDPR does not create a private cause of action for injured data subjects. Enforcement is left to the E.U.'s constituent States.[17] Certain violations carry a maximum fine of the higher of four percent gross annual revenue or 20 million Euros.[18]

II. Emerging U.S. Regimes

Historically, U.S. companies have been subject to a patchwork system of industry-based data-privacy laws.[19] This is likely to change as Congress, States, and municipalities flirt with GDPR-inspired omnibus data-privacy regimes—the forerunner being the California Consumer Privacy Act (CCPA).

A. The CCPA

The CCPA, which becomes effective January 1, 2020,[20] incorporates many of the GDPR's rights with a few notable exceptions.

Similarities to the GDPR.—The CCPA defines personal data similarly to the GDPR.[21] Both contain the right to be forgotten,[22] the right to data portability,[23] the right to be informed of collection and usage,[24] the right to access one's own data,[25] and the right against discrimination for exercising one's rights.[26] It requires data-subjects' consent to use personal data—albeit allowing opt-in-style consent.[27] It contains a breach notification provision.[28] And it mandates that the data handlers it governs use "reasonable" measures.[29]

Differences from the GDPR.—The CCPA targets only large entities and those that use a great deal of California resident data.[30] It does not restrict out-of-jurisdiction transfers. It lacks any requirement to appoint a data protection officer. It does not include a right to correct errors or to contest automated decisions. It limits fines to $7,500 per violation.[31] And it creates a private cause of action: Citizens can recover between $100 and $750 per breach for failure "to implement and maintain reasonable security procedures and practices."[32]

B. San Francisco's "privacy first" policy

On November 6, 2018, San Francisco voted in favor of a "privacy first" policy, requiring the City to develop a regime that protects the data-privacy rights enumerated in the initiative.[33] Those rights include the right to access; the right to informed consent; the right to correct errors; and the right against discrimination.[34]

C. Chicago's proposal

Chicago, too, is entertaining a municipal data-privacy regime: the Personal Data Collection and Protection Ordinance. Although the city council continues to deliberate, the proposal now includes a right to informed consent, a right against discrimination, and a breach notice requirement.[35] It also provides a private cause of action and requires data brokers to register with the City.[36]

D. In Congress

This year, several data-privacy bills are working their way through Congress, each with provisions that resemble those in the GDPR. Although these bills have a long road ahead, they are worth watching. Even if they should fail, they may herald things to come on a national level.

BROWSER Act.—The Balancing the Rights of Web Surfers Equally and Responsibly Act includes a right to opt-in or opt-out consent based on data sensitivity and a right against discrimination.[37]

CONSENT Act.—The Customer Online Notification for Stopping Edge-provider Network Transgressions Act includes a right to opt-in consent, a right against discrimination, and a requirement that internet-based services have "reasonable" data-privacy practices.[38]

MY DATA Act.—The Managing Your Data Against Telecom Abuses Act prohibits the use of "unfair or deceptive act[s] or practice[s] relating to privacy or data security."[39]

Data Security and Breach Notification Act.—The Data Security and Breach Notification Act includes a 30-day breach notice requirement and criminal penalties for willful concealment of a breach.[40]

Consumer Data Protection Act.—The Consumer Data Protection Act requires the Federal Trade Commission to establish minimum data-privacy standards and oversee a national "do not track" list.[41] The Act also contains extreme penalties for violators. Like the GDPR, the Act's maximum fine is four percent of a violator's annual revenue.[42] Moreover, corporate officers can face 20 years in prison for certifying a data-privacy report an officer knows to be false.[43] The Act limits its reach, however, to the biggest of the big: those with $1 billion in annual revenue that hold the personal data of 1 million people, or those that hold the personal data of 50 million people.[44]

Conclusion

The array of regulations to which a data-handling company may be subject is dizzying. And without guiding precedent to light the way, there is an ever-present risk of becoming ensnared. There is one thing, however, that is certain: Those who choose to "wait and see" do so at their own risk.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 J.O. (L 119) (EU) [hereinafter GDPR].

[2] The GDPR does not limit geographically those who may be subject to its provisions.

[3] A controller "determines the purposes and means of the processing of personal data." *Id.* art. 4. A processor "processes" personal data on behalf of a controller. *Id.*

[4] *Id.*

[5] *Id.* art. 7.

[6] *Id.* art. 15.

[7] *Id.* art. 20.

[8] *Id.* arts. 17, 19.

[9] *Id.* art. 16.
[10] *Id.* art. 22.
[11] *Id.* art. 12.
[12] *Id.* art. 12.
[13] *Id.* arts. 44–49. The United States, incidentally, has not been considered to protect private data adequately.
[14] *Id.* art. 33. Controllers must notify within 72 hours. *Id.* Processors must notify their controllers "without undue delay." *Id.*
[15] *Id.* arts. 25, 32.
[16] *Id.* arts. 30, 35.
[17] *Id.* art. 51.
[18] *Id.* art. 83.
[19] *See, e.g.*, Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (regulating telemarketers); Fair Credit Reporting Act, 15 U.S.C. § 1681 (regulating consumer credit reporting agencies); Health Insurance Portability and Accountability Act, 42 U.S. Code § 1320d–6 (regulating healthcare professionals and entities); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–02 (regulating financial institutions).
[20] California Consumer Privacy Act, Assem. Bill 375, 2017-2018 Reg. Sess. § 1798.198 (Cal. 2018) [hereinafter CCPA].
[21] Id. § 1798.140.
[22] Id. § 1798.105.
[23] Id. § 1798.130.
[24] Id. § 1798.100.
[25] Id.
[26] Id. § 1798.125.
[27] Id. § 1798.135. The GDPR requires opt-in consent.
[28] CAL. CIVIL CODE § 1798.29(a).
[29] Id. § 1798.150.
[30] Id. § 1798.140.
[31] Id. § 1798.155.
[32] Id. § 1798.150.
[33] *November 6, 2018 Election Results – Summary*, Department of Elections (stating that the initiative passed).
[34] Revised Legislative Digest Describing and Setting Forth a Proposal to the Voters at an Election to Be Held November 6, 2018, to Amend the Charter of the City and County of San Francisco to Adopt a Privacy First Policy, File No. 180545 (2018).
[35] *Chicago Introduces Data Protection Ordinance*, Hunton Privacy Blog (June 18, 2018).
[36] *Id.*
[37] Balancing the Rights of Web Surfers Equally and Responsibly Act, H.R.2520, 115th Congress §§ 3, 4, 6(12, 15) (2017).
[38] Customer Online Notification for Stopping Edge-provider Network Transgressions Act, S.2639, 115th Congress § 2(b)(2)(B)(iii, vi–vii), § 2(a)(8) (2017).
[39] Managing Your Data Against Telecom Abuses Act, S.964, 115th Congress § 2(b)(1) (2017).

[40] Data Security and Breach Notification Act, S.2179, 115th Congress §§ 5(f), 3(c) (2017).
[41] Consumer Data Protection Act Discussion Draft § 7, at 26, § 6, at 14 (2018). As of writing this, only a discussion draft of the CDPA has been circulated.
[42] *Id.* § 4, at 11.
[43] *Id.* § 1352, at 14.
[45] *Id.* § 5, at 13.