IT'S 10 P.M. DO YOU KNOW HOW SECURE YOUR DATA IS?

Chuck Ragan

Martin Tully

Under new California privacy regulations, you will be obligated to conduct due diligence to answer the question.

As the clock ticks closer to the anticipated July 1, 2023 effective date for new regulations under California's Privacy Rights Act (CPRA), you may draw comfort if you have revised privacy policies, prepared templates and processes for responding to data subject access requests, and updated retention policies in light of data minimization dictates, but how would you answer this question: "Do you know how secure your data is?"

Outsourcing Data Functions Or Moving Data To The Cloud Has Altered Security Risks

In earlier times, when most data was housed on premises, you could respond "as secure as we could reasonably make it with a variety of controls." In 2023, however, the answer necessarily is more nuanced because, by 2022, over 60 percent of corporate data reportedly was stored in a cloud environment (https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/). Is all that data secure? Based on the 2022 IBM Cost of Data Breach report, 45% of data breaches occurred in the cloud and 19% occurred because of compromised systems at a business partner (available for download at https://www.ibm.com/reports/data-breach), so likely some data is not.

New California Regulations To Impose Due Diligence Of Service Providers

Does this situation pose risk of liability under the CPRA? Unfortunately, the answer here is yes, but the risk can be mitigated by smart actions taken before and after the effective date of the CPRA regulations.

The CPRA provides a right of private action for violations that result in compromised personal data (Civil Code § 1798.150(a)) and requires that an organization enter into new agreements with service providers and third parties to which the organization discloses personal data it collects, confirming that the service provider or third party will comply with the obligations of the Act (Id., § 1798.100(d)). Section 7051 of the proposed CPRA regulations --approved by the California Privacy Protection Agency (CPPA) and currently expected to be finalized in April and effective July 1, 2023 -- specifies that certain provisions are to be included in contracts with service providers and contractors.

Among the required elements is that the contract between the business and the service provider or contractor grants the business that owns the data "the right to take reasonable

and appropriate steps to ensure" compliance with the Act, which may include "ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least every 12 months." Section 7051(a)(7).

These requirements are hardly window dressing because the regulations further provide that if the business never exercises the due diligence rights the contracts require, the business may not be able to rely on the defense that it did not have reason to believe that the service provider or third party would misuse the personal information. See Sections 7051(c) and 7053(b). Thus, failure to include the requisite due diligence rights in the contract *and exercise them* could result in the business not only having responsibility for notifying the owner of the data (see https://www.natlawreview.com/article/tech-transactions-data-privacy-2022-report-third-party-data-incidents-preparing-and) but also being held liable as if the breach had occurred within its own systems. *See In re: American Medical Collection Agency, Inc. Customer Data Security Breach Litigation*, No. 19-md-2004, 2021 WL 5937742 at *37 (Dec. 16, 2021).

The regulations approved by the California agency in early February (subject only to review by the state Office of Administrative Law) do not provide guidance on what may constitute adequate cybersecurity audits or risk assessments. Instead, the CPPA has requested comments on proposals and a number of questions to help it frame appropriate further regulations. Comments on those proposals are due by March 27, 2023.

Mitigation Strategies

The first obvious mitigation strategy is to know where your data – and specifically where personal information you collect – resides. This strategy should be part of every organization's information governance program.

The second step is to gather and analyze your contractual arrangements with service providers (cloud and otherwise) who hold personal information you collect and, in light of the CPRA requirements, confirm that you have current written contracts with all such service providers.

The third step is to ensure that the terms or all contracts with service providers or contractors who hold personal information you have collected conform to the requirements of the proposed CPRA regulations.

The fourth step is more difficult and will entail greater consideration, namely, depending on the circumstances and data held by the service provider or third party, developing appropriate due diligence protocols, processes, and schedules. In short, the risk assessments you conduct with service providers and third parties must be reasonable and appropriate to the circumstances, so they may vary. Redgrave LLP can help you with all these strategies regarding appropriate cybersecurity audits and risk assessments.

For additional information on this topic, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.