# Cybersecurity Risk Mitigation in a Post-CCPA/GDPR World

It's official! The California Consumer Privacy Act (CCPA) is now in effect. You've updated your disclosures, considered your contracts, and prepared for requests. At the same time, 2019 saw a large number of fines under the EU's General Data Protection Regulation (GDPR), particularly in relation to cybersecurity. The EU's Network and Information Systems Directive (Cybersecurity Directive) also imposes significant cybersecurity obligations on certain infrastructure and digital services providers. So, what's next? While companies wait for the finalization of the CCPA Regulations and watch for Attorney General enforcement activity beginning July 1, 2020, claims under the private right of action related to data breaches became possible as of January 1, 2020, and GDPR and Cybersecurity Directive enforcement actions and fines are expected in 2020. You can take steps now to mitigate your data breach litigation risk.

## *Phase #1: Define reasonable information security as it applies to your business*

Under the CCPA, a private cause of action is available to individuals whose personal information is subject to a data breach as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. Under the GDPR and Cybersecurity Directive, a similar standard is required, namely of implementing appropriate technical and organizational security measures. Sidley is working with clients to evaluate and assess what reasonable information security may be under the law, as applied to the particular business.

**Phase #1 Deliverables**

Gap Assessment Report of information security policies, controls, and processes against recognized industry standards and laws internationally to help identify opportunities for improvement and memorialize the reasonable information security strategy. The Report can also assess whether third-party IT certification should be considered.

**Timing**

*4–6 weeks*

## *Phase #2: Review key vendor contracts*

Businesses should review key vendor contracts to ensure requirements for vendor contract provisions in the GDPR, Cybersecurity Directive, and CCPA are included and also to assess whether contractual obligations on vendors to report a breach and assist with a breach are appropriate. In addition, contractual provisions limiting liability should be reviewed in light of the increased enforcement actions and private rights of action.

**Phase #2 Deliverables**

Report on updates to key vendor contracts to deal with CCPA, GDPR, and Cybersecurity Directive requirements, and increased liability.

**Timing**

*Estimate dependent on number of key vendor contracts to be reviewed*

## *Phase #3: Update terms of use and other public statements on the reasonableness of the security program*

Applicable governing documents in the United States, such as a website terms of use, present an opportunity to consider arbitration provisions and class action waivers. Businesses should consider whether these documents are appropriate to their business and how best to implement contractual updates.

**Phase #3 Deliverables**

Updated terms or other contractual checklists or provisions with best practice arbitration and class action waiver language in the United States. Consider the risks and benefits of affirmative statements on the reasonable information security program in the privacy policy and marketing materials.

**Timing**
*1–2 weeks*

## *Phase #4: Refresh incident response plan*

Incident response plans are not only expected critical documents for a reasonable information security program; they are also integral to effective incident response. Businesses should review their incident response plan to ensure it is effective, efficient, and appropriate, and considers legal response, privilege, and other litigation defense needs. General updates to cyber and privacy training should also be provided.

**Phase #4 Deliverables**

Sidley will work with your internal IT, legal, compliance, and business teams, as well as your technology consultants, where appropriate, to update your incident response plan and provide cyber and privacy training.

**Timing**
*2 weeks*

## *Phase #5: Update tabletop exercises*

A good incident response program must be practiced to identify opportunities for improvement, vet difficult business decisions in advance, and prepare teams, including outside resources, to work together.

**Phase #5 Deliverables**

Sidley will lead a tabletop exercise.

**Timing**
*2 weeks*
*(or dependent on participant schedules)*

## Contacts


**Colleen Theresa Brown**
Partner
Washington, D.C.
+1 202 736 8465
ctbrown@sidley.com

**Christopher C. Fonzone**
Partner
Washington, D.C.
+1 202 736 8445
cfonzone@sidley.com

**Kate Heinzelman**
Partner
Washington, D.C.
+1 202 736 8416
kheinzelman@sidley.com

**William RM Long**
Partner
London
+44 20 7360 2061
wlong@sidley.com

**Alan Charles Raul**
Partner
Washington, D.C.
+1 202 736 8477
araul@sidley.com


SIDLEY

AMERICA • ASIA PACIFIC • EUROPE

**sidley.com**




MN-12504-01/20