



COVID-19 PRIVACY AND CYBERSECURITY ACTION PLAN FOR BUSINESSES

As the COVID-19 pandemic evolves, companies should not lose sight of the privacy, data protection and cybersecurity implications of the new and sudden digital reality. This Action Plan sets out some key issues and recommendations to consider as your business manages this rapidly developing dynamic and considers protocols to support the workforce and mitigate risk in a transition back to work.

PRIVACY GOVERNANCE

- Develop and maintain COVID-19 privacy protocols that adequately address what, how and when personal data should and should not be collected, used or shared, as well as enterprise-wide security measures to protect the data in transit and at rest. Set data retention policies to maintain data collected for workplace health and safety only for as long as necessary for specific purposes. Revise data privacy and security policies as appropriate, including employee and customer-facing notices that appropriately explain how sensitive data may be collected, used, retained and shared.
- Consider privacy impact assessments, as appropriate, for any new technologies or protocols that may be established to facilitate symptom monitoring and reporting, or exposure alerting.
- Take steps to ensure those assigned to information security and privacy roles collaborate with business leaders and the board and are appropriately involved in key decision-making.
- Consider the organization's position at a global, regional, national and local jurisdiction level and any relevant sector-specific guidance that may necessitate more tailored — or perhaps more flexible — protocols.
- Establish processes to monitor the guidance relevant governmental bodies and regulators are providing with respect to how COVID-19 affects applicable obligations and requirements, enforcement posture and priorities, and pending deadlines.

INFORMATION SECURITY

- Review and update your incident response plan as necessary to address the increased attack surface resulting from working remotely and the potential for key stakeholders to be delayed or unresponsive during an incident. Consider also the need to revise guidance to personnel on how to respond to an incident and ensure multiple backup alternatives for key personnel, with updated contact information, in the event some personnel are sick or indisposed.
- Regularly update patches regarding VPN technologies and other associated software utilized for remote access to company IT resources.
- Limit or disable the use of removable media as appropriate, and ensure that employees report any stolen or lost devices immediately, as there may be a greater chance of theft of employee personal devices when employees are working remotely.
- Deploy and update on a regular basis anti-virus/anti-malware tools used to scan employee computers and shared resources.
- Deploy encryption for data in transit and at rest, and ensure remote wiping capabilities on devices.
- Provide opportunities for online workforce-training refreshers on information privacy and security topics relevant to the organization's business.

REMOTE WORKING

- Consider the need to encourage ongoing remote working even after initial restrictions are lifted.
- Develop a series of “how to” guides and checklists, and distribute to the workforce regular reminders regarding best practices for working remotely to ensure conformity with organization policies and procedures.
- Implement — and take steps to enforce where necessary — written policies on remote working “BYOD,” records management and data loss prevention, information security and privacy, and incident response.
- Regularly remind employees of their confidentiality obligations (including rules for bringing home and disposing of sensitive company or client documents or discussing such information with nonemployees).
- Raise awareness about COVID-19-related phishing emails and recirculate guidance to employees on actions they should take in the event they receive and/or click on a phishing email or experience other types of external threats or cyber-attacks.
- Regularly communicate with the workforce about common remote-working risks to be alert to and about solutions to help protect against unauthorized access to systems and connections, such as company-approved secure computer software and hardware, devices, Virtual Private Networks (VPNs), email and conference lines, and secure WiFi and data storage accounts.
- Determine a protocol for ensuring secure IT asset and records management when onboarding and offboarding personnel remotely, and ensure adequate planning for the preservation and protection of records and IT assets prior to furloughs or layoffs.

BACK TO WORK

- Develop appropriate processes for the implementation of a screening/tracking initiative in line with health and safety needs and the findings of any privacy impact assessment. This should include training for relevant personnel, an assessment of the information security measures and consideration regarding the retention of data.
- Assess whether the ongoing collection of employee or customer health data is necessary and document any risk assessment taken in this regard. Pay particular attention to guidance published by regulators/industry associations and consider whether there is a need to carry out a data protection impact assessment — in particular, when using novel technologies.
- Maintain procedures regarding employee confidentiality, particularly with regard to any medical information collected and information collected on employee contacts (e.g., household members).
- Consider means to ensure that business records created or processed in temporary remote work environments are appropriately returned to work and integrated into records management processes.

RELATIONSHIPS WITH VENDORS AND CLIENTS

- When entering into new vendor agreements or renewing existing agreements, carry out appropriate due diligence and ensure that proper controls are in place to ensure protection of material or sensitive confidential information or personal data, including diligence on key vendors’ business continuity planning.
- Be ready to respond to questions from clients (and others) about your business continuity plans and processes, including privacy and cybersecurity questions. Consider preparing template responses to certain key questions.

MARKETING AND COMMUNICATIONS

- If marketing in Europe, determine whether the communications you are sending to business contacts to stay in touch, or otherwise, would constitute “unsolicited electronic direct marketing” under the e-Privacy Directive and, in turn, require consent.
- If marketing in the U.S., determine whether alternative outreach mechanisms and technologies — such as emails, text communications or auto-dialed calls — raise concerns with respect to CAN-SPAM, the TCPA, telemarketing or other applicable requirements.

COLLECTION OF SENSITIVE DATA

- Determine the legal basis and sensitive-data conditions for the collection, use and sharing of sensitive or potentially protected data, including health data, precise location information and information about contacts (e.g., household members) or personal travel. Consider the appropriateness of consent or legitimate business interest. Where applicable, carry out a GDPR legitimate interest assessment.
- Check jurisdiction-specific privacy and anti-discrimination laws for any applicable restrictions, including on the manner in which data must be maintained and any authorizations that may be required prior to the collection or use of data. Consider the need to liaise with works councils.
- Review privacy notices to ensure that these adequately address the proposed collection of such personal data from each relevant population: employees, customers, facility visitors and other relevant third parties. If not, consider supplemental privacy notices and “just in time” notices to alert them of any automated information collection that might otherwise be considered surreptitious or surprising.
- Limit the collection of sensitive data to the extent possible and consistent with applicable law. Document the organization’s collection, uses and sharing of COVID-19-related health data and any data breaches involving such data.
- Securely maintain and destroy COVID-19-related health data in a manner consistent with company policy and applicable legal requirements.

Contacts

**Colleen Theresa Brown**

Partner
Washington, D.C.
ctbrown@sidley.com
+1 202 736 8465

**Christopher C. Fonzone**

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

**Kate Heinzelman**

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

**William RM Long**

Partner
London
wlong@sidley.com
+44 20 7360 2061

**Alan Charles Raul**

Partner
Washington, D.C.
araul@sidley.com
+1 202 736 8477

SIDLEY

AMERICA • ASIA PACIFIC • EUROPE

sidley.com

Attorney Advertising - Sidley Austin LLP, One South Dearborn, Chicago, IL 60603. + 1 312 853 7000. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/ disclaimer. Prior results do not guarantee a similar outcome. Photos may include Sidley alumni or other individuals who are not Sidley lawyers. Photos may be stock photographs.

MN-13073-05/20