Panorays

Regulation Cheat Sheet

An at-a-glance view of how regulations affect you and your third parties.

REGULATION	PURPOSE	APPLIES TO	KEY POINTS	FINES	VENDOR TAKEAWAYS
CCPA California Consumer Privacy Act Effective Date: 1/1/20	Protects data privacy of California residents	Large organizations that conduct business with California residents	Grants Californians rights over their personal data and right to sue if violated	• **Up to $2,500** per unintentional violation • **$7,500** willful violation of a consumer's rights • Individuals can seek damages of **$100-$750** that can be aggregated into a class action suit	CCPA differentiates between: **Service providers** contracted for specific task using organization's data **Third parties** not contracted by the business, but use organization's data for their own purposes
NY SHIELD ACT Stop Hacks and Improve Electronic Data Act Effective Date: 3/21/20	Protects private information of NY residents	Any person or business owning or licensing computer data that includes private information of NY residents	• Need to implement an ISMS with controls (ex: NIST, ISO 27002) • Complying with GLBA, HIPAA and/or NYDFS = compliance with NY SHIELD ACT	Penalties ranging from **$5,000** per violation to **$20** per failed notification (capped at **$250,000**)	Third-party service providers must maintain cybersecurity practices, including safeguards that are contractually required
GDPR General Data Privacy Regulation Effective Date: 5/25/18	Protects personal data of EU citizens & residents	Any business that works with EU citizens' personal data (including non-EU companies)	• Has spurred a worldwide awareness of the need for digital privacy • Enumerates data subjects' rights • Requires mandatory appointment of a data protection officer (DPO) for companies processing high volume of data	**Up to €20 million or 4% of annual revenue** —whichever is greater	• Data controller determines what info is being processed, and the third party, known in GDPR as the data processor, completes this process on the controller's behalf • The controller is responsible for the processor's compliance
NYDFS New York Department of Financial Services Cybersecurity Regulation 23 NYCRR 500 Effective Date: 3/1/19	Protects sensitive non-public information of NYDFS-regulated NY financial instituitions	Banks, insurance, mortgage companies & financial service institutions that do financial business in NY (even if located elsewhere) & financial institutions' third parties (worldwide)	• Requires very specific cybersecurity assessment requirements: annual PT, biannual vulnerability assessments, periodic risk assessments • DFS-regulated institutions must appoint a CISO	• **Up to $1,000** per violation according to section 408 • Consumer harm need not take place to violate the law and be fined	Mandates a third-party service provider policy to prevent cyberattacks through third parties
EBA European Banking Authority Guidelines Effective Date (new agreements): 9/30/19 Effective Date (existing accounts): 12/31/21	Provides standards to financial institutions with universal rules for all outsourcing	EU banks and other financial firms including e-payment services, electronic money institutions and Fintech providers	• Creates single, standard set of rules for EU banking • Implementation of EBA's risk management improves operational resilience	Financial institutions that don't comply may be sanctioned by the ECB (European Central Bank)	Third-party vendors employed by EU banks and other financial institutions must provide same level of protection as the financial institution
OSFI Office of the Superintendent of Financial Institutions Advisory Effective Date: 3/31/19	Intends to proactively prevent cyber incidents and improve resiliency following a breach	Federally regulated financial institutions (FRFIs) in Canada	Must follow reporting requirements pertaining to high or critical severity technology and cybersecurity-related incidents in a timely manner	Varies based on incident; regulated by OSFI	Mandates: • Identifying material outsourcing arrangements • Monitoring the service providers
PSD2 Payment Services Directive Effective Date: 1/13/18	Intends to make payments more secure in EU by enabling easier payments between members of EU Payments Council, improving consumer protection of EU citizens	Electronic payment services in Europe	Payment service providers must apply SCA (strong customer authentication) for customers making electronic payments for safe user authentication and reduced risk of fraud	Financial institutions that don't comply may be sanctioned by the ECB (European Central Bank)	• Third-Party Providers (TPP) are licensed external parties that can offer certain financial services to consumers • TPPs must comply with security requirements
MAS-TRM Monetary Authority of Singapore-Technology Risk Management Guidelines Effective Date: 8/6/20	Guidelines for technology risk management, including raising cybersecurity standards & strengthening cyber resilience in financial sector	• All financial institutions in Singapore • Service providers and sub-contractors outside Singapore that impact Singapore operations or customers	Requires financial institutions to strengthen security posture by creating cybersecurity policies, standards and procedures, including assessing third parties	Penalties and repercussions: reputational damage, penalties in form of fines, cancellation of license	Requires: • Assessment of service provider and sub-contractors • Outsourcing agreement addressing risks and risk mitigation
FFIEC Federal Financial Institutions Examination Council Guidelines Effective Date: 10/12/05	Standards for banking practices and cybersecurity	Federally supervised US financial institutions	• Financial institutions must follow FFIEC guidelines • Banks and credit unions are audited • Findings are reported and must be remediated	• Penalties depend on severity of non-compliance and which board governs your financial instituition and governing board • May include: cease and desist and restitution orders, fines and court fees, prohibition orders	Senior management is responsible for creating an effective third-party management program to evaluate and manage third-party risk

How Panorays Can Help

Panorays provides a 360-degree view of third parties through discovery and unveiling of the attack surface along with automated questionnaires that check internal policies which correspond to various regulations. This is combined with continuous monitoring and live alerts about any changes to cyber posture. Using these tools, Panorays generates rapid reports that specifically address whether your vendors comply with applicable regulations and what can be done to rectify any issues that may arise.

In addition, Panorays allows you to easily engage with your third parties within the platform. This not only ensures that cyber gaps are mitigated; it provides important compliance documentation that can be helpful when attesting the state of your third-party security.

With these features, Panorays helps you comply with the rigorous third-party cybersecurity requirements of these regulations.

Want to learn more about how Panorays can help you comply with regulations?
Contact your Panorays sales rep or email us at: info@panorays.com