Riscosity

US Telecom : Regulatory Mapping For Data Security And Privacy

A Whitepaper By Riscosity

Data security and privacy are core to making sure forward looking enterprises can protect the information entrusted to them by their end customers. Many laws and regulations apply to telecom providers in the U.S., with a deep focus on incident discovery, event analysis and appropriate remediation and reporting.

In this whitepaper we present a matrix tailored to the requirements for the U.S.-based telecom companies, outlining specific laws and regulations related to data privacy that enforce compliance in tracking third-party data interactions, cataloging financial information, controlling unauthorized data exchange, and reporting incidents:

FTC Laws	CPRA/CCPA	NIST (Applicable Standards)	SOC 2	Other Applicable Laws
1. Keep track of all third-party data interactions involving financial information.				
FTC Safeguards Rule (16 CFR Part 314) Requires oversight of service providers to safeguard customer information.	**CPRA Section 1798.100(b)** Businesses must disclose the categories of personal information shared with third parties.	**NIST SP 800-53 Rev. 5: AC-20** Ensures external system use is monitored and controlled.	**SOC 2 CC1.2** Requires board oversight and governance for tracking data interactions.	**GLBA (Gramm-Leach-Bliley Act)** mandates monitoring and tracking shared financial information.
2. Keep a catalog of what exact financial information is being exchanged.				
FTC Safeguards Rule (16 CFR Part 314) Requires documentation of data handling practices and types of information exchanged.	**CPRA Section 1798.100(a)** Requires businesses to notify customers of specific data being collected and processed.	**NIST SP 800-53 Rev. 5: CM-8** Requires an inventory of system components, including data types.	**SOC 2 CC3.2** Includes risk assessments and cataloging of sensitive data.	**GLBA and HIPAA** (where applicable) enforce documenting and cataloging financial and sensitive information.
3. Have a way to control the exchange of information if something unauthorized is passed through.				
FTC Safeguards Rule (16 CFR Part 314) Requires systems to prevent unauthorized access or transmission of sensitive data.	**CPRA Section 1798.100(d)** Mandates implementation of reasonable security procedures.	**NIST SP 800-53 Rev. 5: AC-3** Establishes access control policies to ensure unauthorized data exchange prevention.	**SOC 2 CC6.1** Implements logical access controls to mitigate unauthorized exchanges.	**PCI DSS compliance requirements** may also apply to financial data, emphasizing controlled exchanges.
4. Have a way to report and alert on any data leak incident.				
FTC Safeguards Rule (16 CFR Part 314) Requires immediate notification to affected parties and regulatory bodies.	**CPRA Section 1798.150(a)** Imposes obligations for breach notification to consumers and regulators.	**NIST SP 800-53 Rev. 5: IR-6** Mandates reporting and logging incidents involving sensitive information.	**SOC 2 CC7.3** Focuses on incident management and notification procedures.	**GDPR Article 33** (if applicable for international operations) requires breach reporting within 72 hours.

Key Laws and Standards in Detail:

1. FTC Safeguards Rule (16 CFR Part 314): Part of the Gramm-Leach-Bliley Act (GLBA), mandates data security for financial information, requiring documented programs, monitoring of third parties, and immediate response to data breaches.

2. CPRA/CCPA: California privacy laws impose strict requirements on data collection, disclosure, and breach notifications. These laws emphasize transparency and consumer rights to know and control data sharing.

3. NIST SP 800-53 Rev. 5: Federal cybersecurity standards provide frameworks for managing third-party interactions, enforcing access control, and establishing reporting protocols.

4. SOC 2: A voluntary compliance standard, but widely used for data privacy in organizations, particularly focusing on security, availability, processing integrity, confidentiality, and privacy.

5. GLBA and PCI DSS: Both applicable in financial contexts, they ensure robust mechanisms for tracking, cataloging, and reporting third-party data interactions involving financial information.

Telecom companies should integrate automated systems for compliance to handle the complexities of these overlapping regulations effectively. Solutions like Data Flow Posture Management enable telecom providers to do more with less. With automation, analysis and remediation in one convenient offering, small GRC, Security, Privacy and IR teams can make the most of their valuable time with automated workflows for detection, analysis and remediation in a single pane of glass.

Sales Contact: sales@riscosity.com
Media Inquiries: marketing@riscosity.com
General Contact: hello@riscosity.com

Riscosity