Chorus Consulting LLC

Colorado Data Privacy Law Compliance Checklist

90% of U.S. Companies Are Not Prepared

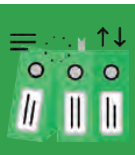
The EU's GDPR made the first big splash in May. The California Consumer Privacy Act passed in June and, when it goes into effect in 2020, will expand U.S. data privacy requirements. But Colorado was the first state to add its own new requirements, and the law went into effect in September.

What The New Colorado Law Requires:

- You must have a written policy explaining how you will dispose of the personal information and follow through on those procedures.
- If a data breach is detected, you must alert consumers that their data has been compromised within 30 days. If more than 500 Coloradans are impacted, the entity must alert the attorney general's office.
- You must take "reasonable" steps to protect the personal information you keep.

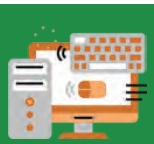
RECOMMENDED ACTIVITIES TO BECOME COMPLIANT

- ✓ Revise your document retention policy and department retention schedules to ensure the immediate destruction of paper and electronic documents containing personal information when that data is no longer necessary (e.g., applications for employment, school admissions, credit, insurance, or property rental; W2, I9, and building security employment documentation; patient medical or financial data; and computer user names and passwords).
- ✓ Map and inventory your organization's document and data storage end points (onsite, offsite, and cloud storage) to understand where documents and data with PII are being saved.
- ✓ Review, and if necessary, renegotiate, and revise contracts with any third-party vendors to require that they implement and maintain reasonable security procedures and practices that are (1) appropriate to the nature of the personal identifying information disclosed and (2) reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure or destruction.
- ✓ Put in place security procedures to protect, track, and report PII (e.g., encrypt documents and data with PII, implement a third-party utility to track the location and status of electronically stored PII throughout the infrastructure).
- ✓ Implement an incident response program to notify affected Colorado residents (and the Colorado Attorney General if more than 500 residents have been impacted) within 30 days after determining that a security breach occurred (this supersedes HIPPA's 60 day breach notification mandate).
- ✓ Perform employee training on this law and its mandate.



Information Governance

Data Security & Compliance



Digital Forensic Services

eDiscovery Services

Advisory Services

Contact Us: (832) 953-5743 | info@chorusconsulting.net | www.chorusconsulting.net