Armstrong Teasdale

DIGITAL TRANSFORMATION

SESSION ONE: NAVIGATING THE PATCHWORK OF CYBERSECURITY AND DATA PRIVACY LAWS | SEPTEMBER 2021

CYBERSECURITY

Federal Trade Commission:

Ask: "What are the industry standards? Are we meeting them?"

- **Patchwork Common Threads**
  - Incident Response Plans (IRPs)
  - Risk Assessments (RAs)
  - Written Information Security Programs (WISPs)
- **IRPs – Key Elements**
  - Phase 1 – Accountability
    - Identify the Incident Response Team (IRT) and its duties
  - Phase 2 – Response Procedures
    - Define incident response procedures and incident severity classifications
  - Phase 3 – Reporting and Notification
    - Identify legal and contractual obligations
  - Phase 4 – Post-incident Response
    - Make sure IRP training, testing and review happens at least every six months
- **RAs – Key Elements**
  - Assess electronic systems at least once every 12 months and any internal and external risks to the security, confidentiality, or integrity of personal or sensitive information and systems
- **WISPs – Key Elements**
  - Evaluate and adjust the WISP in light of any changes to operations or business arrangements

DATA PRIVACY

General Data Protection Regulation (GDPR):

"The law asks you to make a good faith effort to give people the means to control how their data is used and who has access to it."

- **Patchwork Common Threads**
  - There is quite a lot at stake
    - The California Consumer Privacy Act (CCPA) has been amended by the California Privacy Rights Act and becomes operative in January 2023
    - New state laws have passed, Colorado Privacy Act (CPA), Virginia Consumer Data Protection Act (CDPA), and more are being considered
    - Federal laws continue to evolve and enforcement is expanding (e.g., SEC recently settled with app developer for $10 million)
- **Data Privacy Protections and Responses**
  - Privacy "readiness" assessments
    - Applicability analysis of state, federal and international privacy laws
    - Privacy risk assessment
  - Legally defensible GDPR/CCPA compliance programs
    - Review and update existing policies and procedures
    - Prepare data protection impact assessments (DPIAs)
  - Updates to Data Processing Agreements that reflect patchwork, including new EU Standard Contractual Clauses
  - Regulators take cooperation into account
  - Clarity is essential
  - Both legislation and the technology to help address it will continue to evolve

Scott Galt
314.259.4709
sgalt@atllp.com

Romaine Marshall
801.401.1604
rmarshall@atllp.com

Jeffrey Schultz
314.259.4732
jschultz@atllp.com

Dustin Berger
720.722.7197
dberger@atllp.com