Complying with Various Comprehensive Privacy Laws and New York City's Screening Law in 2023

By Anna Mercado Clark and Michael R. Staszkiw
Phillips Lytle LLP

As the new year approaches, businesses should start preparing now for evolving state and local data privacy and protection laws. Businesses should be aware of these key items:

- Comprehensive state privacy statutes set to take effect January 1, 2023;
- New York City's artificial intelligence (AI) screening law to take effect January 1, 2023; and
- The New York State Department of Financial Services' proposed draft amendments to its cybersecurity regulations.

Anna Mercado Clark
Partner

Michael R. Staszkiw
Attorney

Comprehensive State Data Privacy Laws to Take Effect

Next year, five states' privacy statutes will take effect that apply to businesses located within and outside of these jurisdictions: California, Colorado, Connecticut, Virginia and Utah. Generally, these laws provide comprehensive frameworks for processing personal information, impose obligations and rules on businesses that process such information, and set forth consumer rights regarding that information. The California Privacy Rights Act and Virginia's Consumer Data Protection Act both take effect on January 1, 2023, with the remaining three states' laws taking effect later in the year. Each state's law imposes different obligations on businesses and provides different penalties for failing to comply. For example, failing to comply with the California law can result in a $2,500 fine per violation (or $7,500 per violation for intentional violations), while failing to comply with the Virginia law can result in a fine of $7,500 per violation.

New York City's AI Screening Law to Take Effect January 1, 2023

Starting January 1, 2023, New York City employers that use AI decision tools in their hiring processes will need to provide notice to applicants of the use of this technology and publish certain annual audits on the business's website. New York City employers may also be required to make available, upon written request from an applicant or employee, the type of data collected to be used by the AI technology and the company's data retention policy. Failure to comply carries penalties ranging from $500 to $1,500 per violation. Importantly, the law states that each day on which an AI decision tool is used in violation of the law gives rise to a separate violation. New York City employers should take steps now to prepare for the law, or risk the imposition of fines come the new year.

Proposed Amendments to New York State Department of Financial Services Regulations

Recently, the New York State Department of Financial Services released draft amendments to its cybersecurity regulations. Among other proposed changes (which are not currently required), subject businesses will be required to (1) report any ransomware incident within 72 hours, (2) report any paid ransom within 24 hours, and (3) provide a written description of, among other things, why the ransom payment was necessary. The draft amendments also propose certain heightened obligations based on company size and industry practices.

What Can Businesses Do?

To prepare for the new year, businesses may want to consider:

- The applicability of these laws to the business;
- The obligations these laws impose on the business;
- Updating data inventories;
- Updating consumer data access requests response procedures;
- Updating privacy and other policies; and
- Updating vendor contracts.

Phillips Lytle is uniquely situated to provide legal advice and services in the data security and privacy areas due to the technical backgrounds of our practice area partners and decades of successful representation of businesses and financial institutions in data crisis planning and security breaches.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (716) 847-8400 ext. 6466.

Michael R. Staszkiw, CIPP/US, is an attorney at Phillips Lytle LLP and member of the firm's Data Security & Privacy Practice Team. He can be reached at mstaszkiw@phillipslytle.com or (585) 238-2044.