Virtual Cyber Symposium for Nonprofits & Associations

Nonprofit Sector Compliance Conference
December 5, 2023

Presented by Michelle W. Cohen & Nicole Kardell,
Certified Information Privacy Professionals, Privacy & Data Security Practice
Ifrah PLLC
Washington, D.C.

Nonprofits – Why Privacy & Data Security Are Critical

- Privacy and data security are key to nonprofits – Trust even more critical than for-profit companies
  - Donors
  - Supporters & friends
  - Constituents & clients
  - Employees, volunteers
- Nonprofits collect and use personal information which can include:
  - Names
  - Addresses
  - Dates of Birth
  - Donor information
  - Social security/other identifiers
  - Family member info
  - Other demographic details
  - Credit card/payment info

Special Concerns for Nonprofits/Donors

- 80% of organizations do not have any cybersecurity plan according to Board Effect*

- 9 out of 10 organizations do not train staff regularly on cybersecurity

*Board Effect, Nonprofits and Cyberattacks: Key Stats That Boards Need to Know

Data Breaches 2022-23

- 1.35 million people were affected by a private data breach at Broward Health of California in 2022. Source: BoardEffect.2022
- In September 2022, the International Committee of the Red Cross had 500,000 personal data and confidential records compromised
- 54% of organizations were breached through third-parties over a 12-month period. Source: VentureBeat.2022.
- 60% of consumers are less likely to work with a brand that has suffered a data breach (Source: Business Wire - 3/2023).
- Experian breaches by sector – Healthcare (38%), financial services (21%), public sector (16%), retail (12%), education (10%).
- Experian found consumers affected – 78% adults/22% children, with top countries affected: U.S., UK, Canada, Australia, and Mexico

Understanding Privacy & Data Security

- **Privacy**: what data your organization collects, uses, retains and shares/discloses/sells – what is allowed and what you tell the public
  - Data mapping – understanding what is collected, how it is used
  - Privacy policies*
  - Vendor agreements re: confidentiality

- **Security:** how your organization secures the data that you collect, maintain, and share – internal controls, external controls
  - Internal policies and training
  - System security
  - Vendor/third party agreements

Privacy Law Basics - Federal

- **General rule – in the U.S. there is no general federal privacy law (yet)**
- Various bills introduced in Congress – industry has called for a federal standard
- U.S. has sector-specific privacy laws – HIPPA (health info), Gramm-Leach-Bliley (financial institutions), COPPA (children's info – under 13); TCPA (telemarketing); FERPA (student privacy)

Privacy Law Developments - Federal

- U.S. Sen. Catherine Cortez Masto, D-Nev introduced: The DATA Privacy Act – which strengthens protections for American consumers online while ensuring large corporations implement data security and privacy protections. Specifically, the bill would:
  - Allow consumers to request, dispute the accuracy, and transfer or delete their data without retribution.
  - Provide new authorities to state Attorneys General and the Federal Trade Commission allowing them to levy civil penalties for violations.
  - Protect consumer data by requiring three standards to be applied to all data collection, processing, storage, and disclosure:
    - Reasonable: Must be for a legitimate business or operational purpose that is contextual and does not subject an individual to unreasonable privacy risk.
    - Equitable: Data must not be used in a discriminatory way, such as targeting job opportunities based on race or age.
    - Forthright: Businesses cannot engage in deceptive data practices.

- Require businesses to provide users with an easily-accessible opt-out method for personal data collection or sharing. It would also require companies collecting large amounts of personal data to follow data protection standards and to appoint a Privacy Protection Office

Privacy Law Basics - State

- Over about the last 20 years, states focused on breach notifications. Laws address:
  - Who must comply with the law (e.g., businesses, data brokers, government entities)
  - What is “personal information” under their law (e.g., name, SSN, drivers license, account numbers, etc.)
  - What constitutes a breach (e.g., unauthorized acquisition of data)
  - Notification requirements (e.g., timing or method of notice, who must be notified)
  - Exemptions (e.g., for encrypted information)
  - **Yes, apply to nonprofits**
- Some states have developed more fulsome laws. The most comprehensive being….

Privacy Law Developments - California

California: California Consumer Privacy Act (CCPA) (effective January 2020), as amended by California Privacy Rights Act (effective January 2023)

- *Generally, does not apply to nonprofit organizations. However, nonprofits who contract with businesses that are subject to CA law may need to comply with certain requirements.*
- May apply to nonprofits that "control or are controlled by" or that "shares common branding" with a business may be subject to the CCPA.
  - "control" means ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a business; control in any manner over the election of many of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company.
  - "Common branding" means a shared name, servicemark, or trademark.
- NOTE: California has several privacy laws, including their "Shine the Light" law, which applies if you have more than 20 employees.

Privacy Law Developments – New York

- Nonprofit organizations (and others) that receive, collect or otherwise possess private information about New York residents must comply with the New York SHIELD Act

- Two components:
  - covered entities must adopt a comprehensive cybersecurity data protection program to safeguard "private information," and
  - covered entities must comply with data breach notification requirements

Privacy Law Developments – New York

The SHIELD Act requires any person or business that maintains private information to adopt administrative, technical, and physical safeguards. The act lists some (non-exhaustive) safeguards:

Reasonable administrative safeguards include:

- designating one or more employees to coordinate the security program
- identifying reasonably foreseeable internal and external risks
- assessing the sufficiency of safeguards in place to control the identified risks
- training and managing employees in the security program's practices and procedures
- selecting service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract
- adjusting the security program in light of business changes or new circumstances

Reasonable technical safeguards include:

- assessing risks in network and software design
- assessing risks in information processing, transmission and storage
- detecting, preventing, and responding to attacks or system failures
- regularly testing and monitoring the effectiveness of key controls, systems, and procedures

Reasonable physical safeguards include:

- assessing risks of information storage and disposal
- detecting, preventing, and responding to intrusions
- protecting against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of information
- disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed

Privacy Law Developments – New York

- Some relief for small businesses - deemed compliant with the SHIELD law's data privacy requirements if it has adopted "reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

STATE PRIVACY LAWS – SEVERAL NEW LAWS

- The past two years have seen an **uptick in state privacy legislation**
- Currently, **13 states** have enacted privacy laws:
  - California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, Virginia
- Most of these states' privacy frameworks explicitly exempt non-profits from compliance requirements except:
  - **Colorado, Delaware and Oregon**

STATE PRIVACY LAWS – SEVERAL NEW LAWS

Colorado: Colorado Privacy Act (effective July 2023)

- Threshold requirements to trigger compliance:
  - If, during a calendar year, you control or process personal data of **100,000 or more Colorado residents**; or
  - If you both derive revenue or receive discounts from selling personal data and process or control the personal data of **25,000 or more Colorado residents**.

STATE PRIVACY LAWS – SEVERAL NEW LAWS

Delaware: Delaware Personal Privacy Act (effective January 2025)

- *Only exempts certain nonprofit organizations in insurance crime and involved in protection of victims/witnesses of child abuse, domestic violence, human trafficking, sexual assault, violent felony, or stalking.*
- Threshold requirements to trigger compliance:
  - If you conduct business in Delaware or produce products or services that are targeted to residents of Delaware and that during the preceding calendar year did any of the following:
    - Controlled or processed the personal data of **35,000 or more consumers**, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or
    - Controlled or processed the personal data of **10,000 or more consumers** and derived more than **20 % of their gross revenue** from the sale of personal data.

STATE PRIVACY LAWS – SEVERAL NEW LAWS

Oregon: Oregon Consumer Privacy Act (effective July 2024; application to non-profits July 2025):

- *Only exempts certain nonprofit organizations involved in insurance fraud detection/prevention and involved in programming to radio or television networks.*
- Threshold requirements to trigger compliance:
  - If you conduct business in Oregon or provide products or services to residents of Oregon and that during a calendar year you control or process:
    - The personal data of **100,000 or more consumers**, personal data from 100,000 or more devices that identify or link to or are reasonably linkable to one or more consumers, or personal data from a combination of 100,000 or more consumers and devices; or
    - The personal data of **25,000 or more consumers**, while deriving **25 %** or more annual gross revenue from selling personal data.

STATE PRIVACY LAWS – GENERAL REQUIREMENTS

- **Consumer Rights:**
  - General. The right to access, delete, and correct personal data
  - Data portability. The right to obtain a portable and usable copy of the data.
  - Opt-outs. The right to opt out of the sale of personal data or its use for targeted advertising or certain kinds of profiling
  - *No private right of action*
- **Entity Obligations:**
  - Transparency. Privacy notice discussing collection and use of data
  - Consent. Obtain consent for processing sensitive personal data (data of child under 13, data revealing race, ethnicity, religion, mental/physical health, sexual activity, sexual orientation, citizen status, biometric data)
  - DPAs. Conduct Data Protection Assessment before selling personal data, processing "sensitive data," or processing personal data that could result in harm, including financial
  - Universal Opt-Outs. Accept opt-out requests through universal opt-out mechanisms starting on July 1, 2024
- **Exemptions:** If subject to federal laws covering data requirements (e.g., GLBA, SEC, FAA, HIPPA, FCRA, COPPA

GDPR

- Europe *does* have a central privacy law – **GDPR**
- U.S. nonprofits raising money in the E.U. or providing services to EU citizens and collect personal data must follow the GDPR
- GDPR applies to nonprofits and has several requirements, including:
  - Data breach notification within 72 hours
  - Regulatory bodies can impose substantial fines.

GDPR

- The GDPR provides the following rights for individuals:
  - The right to be informed
  - The right of access
  - The right to rectification
  - The right to erasure
  - The right to restrict processing
  - The right to data portability
  - The right to object
  - Rights in relation to automated decision making and profiling

GDPR/Nonprofit Enforcement

- Belgian Data Protection Authority fined nonprofit (May 2020)
  - Individual continued to receive promotional materials after objecting to processing of contact details for direct marketing and had requested erasure of data from database
  - Unsolicited postal communication sent by nonprofits (including fundraising) qualify as “direct marketing” under GDPR.
  - Organization did not (a) immediately stop the processing after he exercised right to object and right to be forgotten – continued for at least 5 months after individuals request and 3 months after complaint to Belgian DPA
  - Did not have a valid legal basis for processing the personal data for direct marketing
    - Did not obtain consent
    - Claimed legitimate interest – but ruled overridden by individual’s rights – more than 7 years since donation

Privacy Policies

- Black letter privacy law – say what you do and do what you say

- Privacy Policies – promises that are enforced
  - For-profit companies – FTC
  - Nonprofit organizations – State Attorney Generals

May 2020

Blackbaud Breach – Case Study

- Blackbaud – cloud computing provider
- 25,000 nonprofits, schools, and other organizations.
- Breach – discovered May 2020/notified domestic and international customers July 2020
- Affected parties – donors, students, patients
- Lawsuits – vs. Blackbaud and customers (Harvard, Lower East Side Tenement museum, others)

Blackbaud – Case Study

- Many nonprofits received notification from Blackbaud concerning the ransomware attack.
- What we recommended
  - Review what Blackbaud said was accessed
  - Independently determine what Blackbaud services the organization used
  - Determine what type of data stored in Blackbaud and possibly accessed
  - Assess individuals who may be affected – including state of residence
  - Analyze state data breach laws and whether info triggers reporting
  - Don’t forget Europeans/citizens of other countries
  - Public announcements - company judgment call

Blackbaud

- October 2023: Blackbaud agreed to pay $49.5 million to settle claims brought by the attorneys general of 49 states and Washington, D.C., related to the 2020 data breach that exposed sensitive information from 13,000 nonprofits.

Cybersecurity Insurance

Cyber insurance policies can cover losses from:

- breaches affecting a nonprofit's own information
- losses affecting third parties' information (such as clients and donors).

What Kind of Losses:

- data breach notification costs
- content repair, (e.g, hacked website)
- communications consultants for reputation repair
- business interruption

Insurance carrier will typically ask:

- types of personal information stored or processed – e.g., bank account, credit card, driver's license, protected health information, social security numbers
- disclosures about prior losses due to unauthorized access, use, virus, data breach, theft, or other electronic security events.
- complaints/proceedings regarding privacy rights
- use of firewalls/software updates/virus scans
- restricted access to sensitive data
- access termination/removal of outdated accounts
- physical security to restrict access to computer systems and sensitive records
- business continuity plan in event of incident
- system back up and recovery procedures
- encryption of sensitive data
- designated person/group responsible for IT security and compliance
- information security or privacy compliance evaluation
- training of employees including reporting of suspected security incidents

SELECTED RESOURCES

- National Conference of State Legislatures data breach chart: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
- International Association of Privacy Professionals: https://iapp.org/
- FTC resources - https://www.ftc.gov/tips-advice/business-center/selected-industries/non-profits

THANK YOU!
Questions?

Michelle Cohen

Email: michelle@ifrahlaw.com
(202) 524-4144
Twitter: @MichelleWCohen

Nicole Kardell

Email: nkardell@ifrahlaw.com
(434) 249-5330