PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Data Privacy for Nonprofits

Candice Decaire

March 16, 2016

PRO BONO™
PARTNERSHIP / ATLANTA

KILPATRICK TOWNSEND

Mission of Pro Bono Partnership of Atlanta:

To maximize the impact of pro bono engagement by connecting a network of attorneys with nonprofits in need of free business legal services.

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Pro Bono Partnership of Atlanta Eligibility & Other Information

- In order to be a client of Pro Bono Partnership of Atlanta, an organization must:
  - ✓ Be a 501(c)(3) nonprofit.
  - ✓ Be located in or serve the greater Atlanta area.
  - ✓ Serve low-income or disadvantaged individuals.
  - ✓ Be unable to afford legal services.
- *Visit us on the web at* www.pbpatl.org
- We host free monthly webinars on legal topics for nonprofits
  - ✓ To view upcoming webinars or workshops, visit the Workshops Page on our website
  - ✓ Join our mailing list by emailing rla@pbpatl.org

Legal Information:

✓ This webinar presents general guidelines for Georgia nonprofit organizations and should not be construed as legal advice. Always consult an attorney to address your particular situation.

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

DATA PRIVACY for NONPROFITS

- data privacy responsibilities and risks;
- applicable laws and standards;
- components of a privacy policy;
- prudent information governance;
- data breach and incident response;
- risk mitigation and “cyber-liability” insurance

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Privacy of Personal Information

- What is “personal information”?
- **information that can be used to identify an individual**
- Personal Data Notification and Protection Act defines “**sensitive personally identifiable information**”
  - FTC can amend to include combinations of information or particular pieces of information determined to be sensitive personally identifiable information

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Sensitive personally identifiable information:

First and last name, or initial and last name + any two of:

- Home address, phone number
- Mother's maiden name
- Birthday (month, day , year)
- SSN, driver's license number, Passport number, other government-issued ID number
- Unique biometric data (e.g., fingerprint, voice print)
- Unique account identifier
- User name + password for online account
- Any combination of: first, last name; unique account identifier; access code / password

PRO BONO™
PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

- Necessary to collect, store, and use personal information relating to members, donors, employees, business partners, and constituents to conduct core functions -
- But collecting, storing, and using such information presents privacy risk
- Essential to develop controls to mitigate that risk

PRO BONO™ PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

- Some privacy laws exempt nonprofit organizations
- But your volunteers, donors, business partners, constituents expect that you will keep their information safe
  - ✓ Critical to preserve reputation and good will by managing privacy risks such as unauthorized data destruction, modification, retention, disclosure, and use
  - ✓ Balance the need to collect and store information against increased risk, and cost and effort of safeguarding information

Fair Information Practice Principles (FIPPs)

- Notice / Awareness
  - ✓ Privacy policy – who collects what, how, and why
- Choice / Consent
  - ✓ Consent for use of information, opt in or out
- Access / Participation
  - ✓ Individuals can access, review, correct their data
- Integrity / Security
  - ✓ Ensure data quality, safety
- Enforcement / Redress
  - ✓ Comply with law, regulations, industry practice

What are the rules?

- Patchwork of laws in the United States; no single regulatory authority
- Federal regulation, generally enforced by FTC
  - ✓ specialized for healthcare, financial information, immigration, travel records, telemarketing
- State laws re: unfair and deceptive trade practices, identity theft, data breach
- Industry self-regulation (e.g., Payment Card Industry Data Security Standards)

PRO BONO™
PARTNERSHIP / ATLANTA

KILPATRICK TOWNSEND

How do I comply?

- Define the problem:
  - ✓ what personal information do you collect?
  - ✓ what rules apply?
- Build policies, practices
  - ✓ Consider privacy impact assessment
- Communicate
  - ✓ Internal training, external notification
- Stay current
  - ✓ Monitor, update, adapt

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Document a Privacy Policy:

- Consider:
  - ✓ Sensitivity of the information
  - ✓ Quantity of information
  - ✓ Scope of distribution
  - ✓ Format (electronic? paper?)
  - ✓ Location, method of storage
- Using third party vendors, service providers?

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Core Components of Privacy Policy:

- Notice – why are you collecting the information, how are you using it? Will you be sharing it?
- Choice and consent – get permission to use the information for specific purpose(s)
- Minimization – limit collection and use to what is relevant, reasonably necessary
- Data accuracy – ensure information is correct, establish procedures to permit individuals to review and correct their information

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Core Components:

- Data retention – don't keep information any longer than necessary; ensure secure disposal
- Data security – appropriate policies and practices, physical measures, technical controls
- Contracts with vendors, service providers –require appropriate measures to protect personal information
- Notification of changes to policy
- Contact information for questions about policy

Don’t stop at the policy:

- Conduct regular privacy / security training
- Confirm training and attendance
- Ensure that employees / volunteers know:
  - ✓ How to respond to inquiries about privacy policies
  - ✓ When consent is required and how to obtain it
  - ✓ How to recognize and respond to requests for personal information
  - ✓ How to handle complaints about protection of personal information

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Access to Personal Information:

- Restrict access to need-to-know
- Password-restricted access for computer systems
- User IDs and passwords unique to each user
- Locks for filing cabinets
- Track access
  - ✓ Know who has access to what; log access
  - ✓ Ensure access permissions and log are updated

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Social Media:

- Do you use social media? Mention names or use pictures of volunteers, others?
- Need to address:
  - ✓ Content - control organization's reputation
  - ✓ Permissions / waivers
  - ✓ Terms and conditions of social media site
- Prudent to have explicit social media policy
  - ✓ Authorized users agree to terms and conditions
  - ✓ Designate point person to approve posts

Email & CAN-SPAM: OTHER CAN SPAM

- CAN-SPAM Act
  - ✓ Can apply to nonprofits sending emails promoting commercial products or services
  - ✓ Requires that recipients have right to say “no more”
  - ✓ Harsh penalties for violation
- Use mailing lists? Acquired from whom? Know whether source of list has eliminated individuals who do not want their names to be shared?

Credit Card Processing:

- Payment Card Industry Data Security Standard (PCI DSS 2.0)
- Must comply to accept payment cards or to store, process, and transmit cardholder data
  - ✓ https://www.pcisecuritystandards.org/
  - ✓ PayPal for Nonprofits: https://merchant.paypal.com/cms_content/US/en_US/files/merchant/paypal_nonprofit_faqs.pdf

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Keep in mind, additional requirements:

- Telephone or text campaigns
- Healthcare information
- Financial information
- Education records
- Immigration, travel information
- Information collected online from children
- Information transferred to or from other countries

Data breach:

- Laws in 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require notification of security breaches of information involving personally identifiable information
- Security breach laws typically have provisions about:
  - ✓ who must comply with the law
  - ✓ definitions of covered “personally identifiable information”
  - ✓ what constitutes a breach (e.g., unauthorized acquisition of data)
  - ✓ requirements for notice (e.g., timing, method, who must be notified)
  - ✓ exemptions (e.g., for encrypted information)

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Georgia's Data Breach Law:

- must notify affected Georgia residents as soon as possible through mail, telephone, or electronic means
- if the security breach affects more than **100,000** people, or the cost of notification exceeds **$50,000**, other means of notification can be used (e.g., public service announcements)
- breach affecting more than **10,000** people needs to be reported to all credit reporting agencies
- safe harbor for encrypted information

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Georgia's Definition of personal information:

- (1) name or other identifying info, AND
- (2) one or more of:
  - ✓SSN;
  - ✓driver's license number; or
  - ✓account number, credit card number, debit card number, especially if accompanied by PIN, password, or access codes
  - ✓Numbers, access codes, other information sufficient to attempt identity theft

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Georgia requires notification of breach:

- Any information broker or data collector that maintains computerized data that includes personal information of individuals
- Must give notice of breach of security to person who unencrypted information was, or is reasonably believed to have, acquired by unauthorized person
- “in the most expedient time possible and without unreasonable delay”
- Must also take any steps necessary to “restore the reasonable integrity, security, and confidentiality of the data system”

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Georgia law also applies to services provider:

- Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own
- shall notify the information broker or data collector of any breach of the security of the system
- within 24 hours following discovery,
- if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Minimize chances of a data breach:

- Consolidate data and limit storage sites; encrypt data
- Delete old or irrelevant data; ensure proper disposal of records, devices
- Regularly update software
- Train your employees
- Have a BYOD policy and enforce it
- Consider a professional privacy/security audit

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Make a plan, in case of breach:

- Designate someone to secure the breach, identify causes and ways to prevent
- Identify your legal obligations - determine who to notify, and how fast you have to do; make a list
- Designate someone to be responsible for notifications
  - ✓ Set up for website notification, consider phone line or email to take questions from those affected by breach
- Vendors, service providers involved?
  - ✓ insurance? Indemnification?
- Be familiar with your insurance coverage, requirements

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Risk mitigation: information governance

- Back to the privacy policy
  - ✓ Know what you collect
  - ✓ Know who is responsible
  - ✓ Ensure your “customers” and employees are informed
  - ✓ Don’t promise too much
- Manage risks with visibility
- Maintain and update security measures
- Have an incident response plan

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Cyber-liability insurance:

- General liability insurers may exclude coverage for compromised data and for costs of responding to and remediating the data breach or violation
- Consider obtaining coverage for common risks:
  - ✓ hacker
  - ✓ “ghost in the machine”
  - ✓ “oops”
  - ✓ “blogger”

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Some cyber-liability insurance issues:

- What is coverage territory? Deductibles? Policy limits? Sublimits for data breach, remediation?
- Vendors, service providers – are you an "additional insured"?
- Coverage for fines, penalties?
- Check the exclusions (remember, you want to cover the "oops," etc.)

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

In sum:

- Know your responsibilities / risks:
  - ✓ Determine whether / what personal information you collect and how it is stored and used
  - ✓ Be transparent about your policies; obtain consent
  - ✓ Know the rules (and follow them)
- Establish and regularly update your security
  - ✓ Policies, practices, training, technology
  - ✓ Consider obtaining impact assessment
- Further protection - contracts, insurance

PRO BONO PARTNERSHIP/ATLANTA

KILPATRICK TOWNSEND

Thank you!

Any questions?

Data Privacy for Nonprofits

Candice Decaire

March 16, 2016

PRO BONO™
PARTNERSHIP / ATLANTA

KILPATRICK TOWNSEND

For More Information:

If you would like more information about the services of Pro Bono Partnership of Atlanta, contact us at:

www.pbpatl.org
info@pbpatl.org
404-407-5088