Welcome

Our Presentation

Will Begin at 12pm

- All viewers are muted. Audience cameras cannot be turned on.
- Who's with us today? We invite you to share your nonprofit's name in the chat box.

PRO BONO™
PARTNERSHIP/ATLANTA

Practical Data Privacy Guidance for Small Nonprofits

PRO BONO™

PARTNERSHIP / ATLANTA

Jason A. Bernstein

Barnes & Thornburg

February 26, 2026

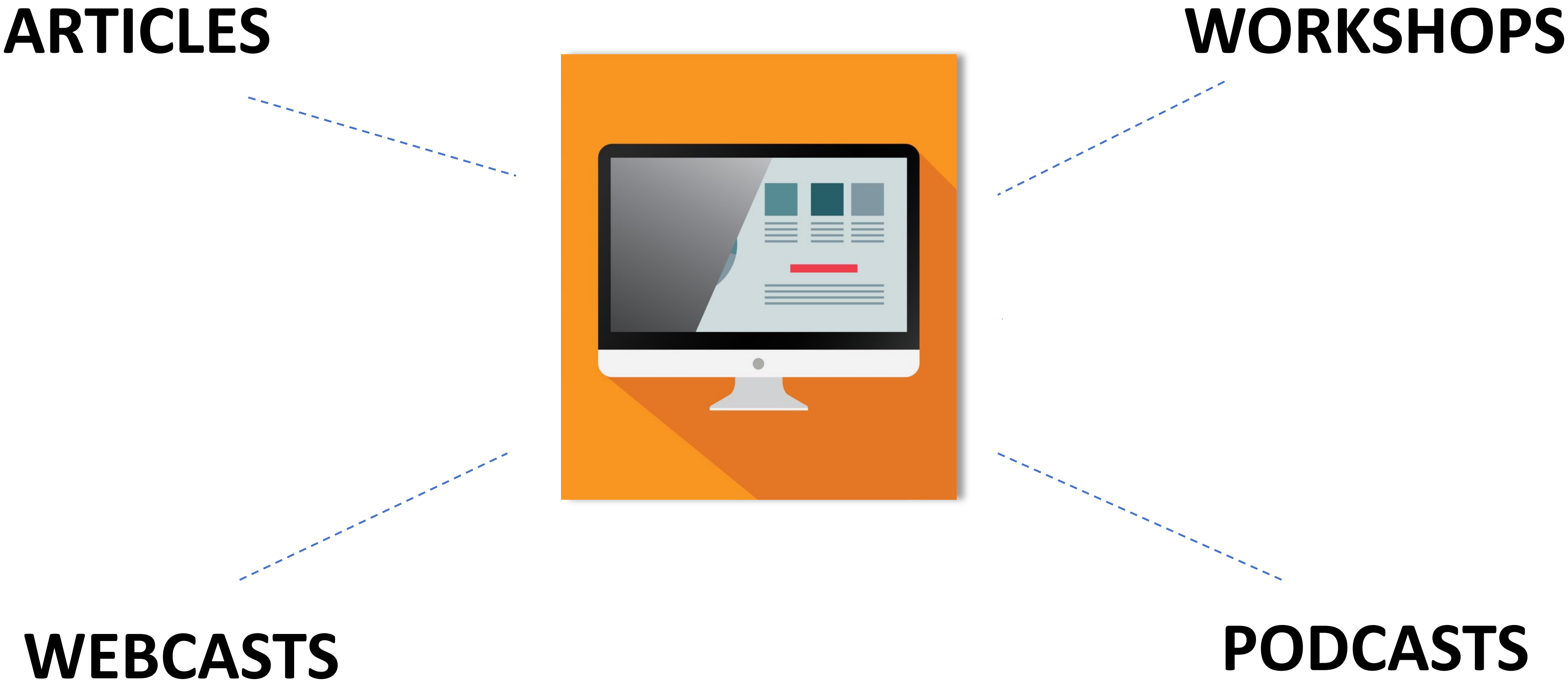
Mission of
Pro Bono Partnership of Atlanta

To provide free legal assistance to community-based nonprofits that serve low-income or disadvantaged individuals.

We match eligible organizations with volunteer lawyers from the leading corporations and law firms in Atlanta who can assist nonprofits with their business law matters.

PBPA Learning Center for Georgia Nonprofits

www.pbpatl.org/resources



ARTICLES

WORKSHOPS

WEBCASTS

PODCASTS

PRO BONO™
PARTNERSHIP/ATLANTA

Client Criteria

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.
- Employ at least one paid staff person.

Visit our website at www.pbpatl.org to apply.

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

Agenda

How Data Affects You

And

How You Affect Data

Agenda

- What is PI?
- Collection
- Storage
- Consents
- Use (“Processing”)
- Disclosure
- Transfer
- Disposal
- Training
- Compliance

What is “Personal Information”(PI)?

Personal information is any data (either alone or in combo with other data) that identifies (or can be used to identify) an individual, e.g.:

Name

Citizenship/Immigration Status

Address

Email

Phone

SSN

Date of Birth

Device Info

Geolocation

Health/Financial Info

Sensitive PI

- Race/ethnicity
- Political opinions
- Sex life/orientation
- Health
- Trade union membership
- Biometric
- Genetic

Collection – Where Does PI Come From?

From:

- Donors
- Volunteers, employees, board members
- Clients/customers
- Website visitors
- Conference and meeting attendees
- Data vendors
- Research partners

Sources:

- Website, mobile app, email, phone, mail, in person

Collection and Storage

- Data is an asset --- and a liability/risk
- Data Minimization:
  - Collect only PI that is necessary for your needs/purposes
  - Don’t collect PI if you don’t really need it (e.g., SSN)
- Don’t store PI in a shared folder or drive that everyone can access
- Store it in a safe and secure place (internal server, cloud, offline)
- **USE MULTI-FACTOR AUTHENTICATION**
- Restrict access to just those who need it
- Have a set of internal policies covering data security

Collection – AI Notetaking

- Do not record conversations with your attorneys
- Before recording any sensitive conversation, find out if the vendor (e.g., Zoom) will have access to the transcription
- Get consent from those being recorded
- Review for accuracy

Consents

- Needed so that privacy policy and terms of use are enforceable
- Europe, UK, Switzerland require obtaining consent before collecting PI (i.e., “opt-in”) (unless legitimate interest)
- Consent requires
  - Proper notice
  - Active (not passive) action from user indicating consent
- Do not use pre-checked boxes for anything
- Parent/guardian consent needed for those <18

Consents

- Have consent "gate" at all data collection points before PI is submitted
- Clear acceptance language:
  - □ By checking the box, I acknowledge I have read and agree to be bound by the Terms of Use and Privacy Policy.
  - By clicking on the Submit button below, I acknowledge I have read and agree to be bound by the Terms of Use and Privacy Policy.
- Don't minimize presentation of the language
- You must allow individuals to withdraw consent at any time

Use ("Processing")

- Know what you do with data and why
- Different areas of your organization use different data in different ways
  - Membership list management
  - Donation and fundraising management
  - Research
  - Client service
  - HR
  - Finance
  - Marketing
  - Event management

Disclosure

Who do you disclose PI to?

- Grantors
- Research partners
- Vendors
- Gov’t agencies
- The public

Transfer

- In the event of a merger or sale of the organization, PI is often transferred

Disposal

- Delete PI when it’s no longer needed
- If a hacker gets into your system and takes PI you’ve stored, that data is now a liability

Training

The Shampoo Approach

Educate

Train

Rinse

Repeat

Compliance – With…

What do you have to comply with?

- Laws and regulations
  - Medical – HIPAA
  - Financial – Gramm-Leach
  - Children – COPPA, FERPA
  - Texting – TCPA (for marketing purposes)
  - Website – ADA
  - Foreign: EU's GDPR, Canada's PIPEDA, etc.
- Payment Card Industry DSS standards
- Grantors
- Contractual obligations (vendors and customers)
- Research partners
- Your own privacy policy

Compliance Steps

- Determine what you must comply with
- Determine what PI you collect and who from
- Do you have the right policies in place?
- Do as you say and say as you do
- Do a gap analysis of what is versus what must be
- Revise or implement policies/procedures
- Train staff

What You Should Have and Do

- Website privacy policy
- Proper consent “gates” when collecting PI
- Internal policies and procedures for managing data
- Training schedule
- Look at your agreements involving data

Summary

- Know what PI you collect and from what sources
- Know what your organization does with PI, who it is disclosed to, and how it is stored/deleted
- Have data security measures in place
- Know what you have to comply with
- Train personnel to strengthen cyber defenses

Bonus!

Personal Cyber Hygiene Defense Tips

1. **Freeze your credit!**
2. Use two-factor authentication
3. Backup routinely – the best defense to ransomware lockup attacks
4. Use strong passwords-passphrases (or a password manager)
5. Use different passwords – junk vs. important accounts

Personal Defense Tips:
Cyber Hygiene

6. Change your passwords regularly
7. Hover--Don’t click on links in email to see if they are legit
8. Promptly install software security updates
9. Don’t use public Wi-Fi with your laptop unless with a VPN
10. Disconnect external backup drives to avoid lockup

Questions?

Pro Bono Partnership of Atlanta
www.pbpatl.org

As a nonprofit ourselves, PBPA relies on donors to continue providing free legal assistance to organizations like yours. If you're able to give, please consider donating to help us keep serving Georgia's nonprofits.

PRO BONO
PARTNERSHIP/ATLANTA