



# LIST BAZAAR

MAY 12, 2022

The Legend returns...

# Our Session Partner!

---

mmidirect

# Session

---

## **Data Privacy Update: What List Professionals Need to Know**

**Jon Dartley**

Of Counsel, Perlman & Perlman

**Britt Vatne**

President, Account Management, Adstra

# The State of Play

## *State Regulations & Privacy/Cybersecurity Best Practices*

*Presented by*  
**Jon Dartley, Ph.D**  
*Attorney, Perlman & Perlman, LLP*

*Please be advised that the information provided in the presentation is for general information purposes only and is not to be construed as legal advice.*



# US State Privacy Legislation Tracker

## Comprehensive Consumer Privacy Bills

STATE	LEGISLATIVE PROCESS	STATUTE/BILL (HYPERLINKS)	COMMON NAME	CONSUMER RIGHTS										BUSINESS OBLIGATIONS		
				Right of access	Right of rectification	Right of deletion	Right of restriction	Right of portability	Right to opt out of sales	Right against automated decision making	Private right of action	Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments	Prohibition on discrimination (exercising rights)	Purpose/processing limitation
LAWS SIGNED (TO DATE)																
California		<a href="#">CCPA</a>	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	X		X		X	X		L	16	X			X
		<a href="#">Proposition 24</a>	California Privacy Rights Act (2020; effective Jan. 1, 2023)	X	X	X	S	X	X	X	L	16	X	X	X	X
Colorado		<a href="#">SB 190</a>	Colorado Privacy Act (2021; effective July 1, 2023)	X	X	X	P	X	X	X-		S/13	X	X	X	X
Virginia		<a href="#">SB 1392</a>	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)	X	X	X	P	X	X	X-		S/13	X	X	X	X
Utah		<a href="#">SB 227</a>	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)	X		X	P	X	X			13	X		X	

ACTIVE BILLS

Alaska		<a href="#">HB 159</a>	Consumer Data Privacy Act	X		X		X	X		X	18	X		X	X
		<a href="#">SB 116</a>	Consumer Data Privacy Act	X		X		X	X		X	18	X		X	X
		<a href="#">HB 222</a>	Alaska Consumer Information Protection Act	X	X	X	S	X	X		L	16	X		X	X
Connecticut		<a href="#">SB 6</a>		X	X	X	P	X	X	X-	S/16	X	X	X	X	X
Louisiana		<a href="#">HB 987</a>	Louisiana Consumer Privacy Act	X		X	P	X	X		13	X		X		
Massachusetts		<a href="#">S 2687</a>	Massachusetts Information Privacy and Security Act	X	X	X	S	X	X		L	16	X	X	X	X
		<a href="#">H 4514</a>	Massachusetts Information Privacy and Security Act	X	X	X	S	X	X		L	16	X	X	X	X
Michigan		<a href="#">HB 5989</a>	Consumer Privacy Act	X	X	X	P	X	X	X-	S/18	X	X	X	X	X
New Jersey		<a href="#">A 505</a>	New Jersey Disclosure and Accountability Transparency Act	X	X	X	X	X	IN	X	X	ALL	X	X		X
		<a href="#">S 332 *</a>		X	X				X				X		X	
		<a href="#">A 1971 *</a>		X	X				X				X		X	
New York		<a href="#">A 680B</a>	New York Privacy Act	X	X	X	X	X	IN	X	L	ALL	X	X	X	X
		<a href="#">S 6701A</a>	New York Privacy Act	X	X	X	X	X	IN	X	L	ALL	X	X	X	X
		<a href="#">A 6042</a>	Digital Fairness Act	X		X		X	IN	X	X	ALL	X	A	X	X
		<a href="#">S 567</a>		X					X		X	16	X		X	
North Carolina		<a href="#">A 3709</a>		X					X		X	16	X		X	
		<a href="#">S 569</a>	Consumer Privacy Act	X	X	X		X	X	X-	X	S	X	X	X	X
Ohio		<a href="#">HB 376</a>	Ohio Personal Privacy Act	X	X	X	P	X	X		13	X		X	X	
Pennsylvania		<a href="#">HB 1126</a>		X		X		X			L	16	X		X	
		<a href="#">HB 2202</a>	Consumer Data Privacy Act	X	X	X	P	X	X	X-	16	X		X	X	
		<a href="#">HB 2257</a>	Consumer Data Protection Act	X	X	X	P	X	X	X-	S/18	X	X	X	X	X
Rhode Island		<a href="#">H 7917</a>	Rhode Island Information Privacy Act	X	X	X	X	X	IN		X	ALL	X		X	X
Vermont		<a href="#">H 160</a>		Only short-form bill available												
		<a href="#">H 570</a>		Only short-form bill available												

Minnesota					<a href="#">HF 1492</a>	Minnesota Consumer Data Privacy Act	X	X	X	P	X	X	X~		S/13	X	X	X	X
Mississippi					<a href="#">SB 2330</a>	Mississippi Consumer Data Privacy Act	X		X			X		L	16	X		X	
Nebraska					<a href="#">LB 1188</a>	Uniform Personal Data Protection Act	X	X				*	*		*	X	X	X	X
					<a href="#">HB 1602</a>	Oklahoma Computer Data Privacy Act	X		X		X	IN			ALL	X		X	
Oklahoma					<a href="#">HB 3447</a>	Uniform Personal Data Protection Act	X	X				*	*		*	X	X	X	X
					<a href="#">HB 2969</a>	Oklahoma Computer Data Privacy Act of 2022	X		X		X	IN			ALL	X		X	X
					<a href="#">HB 1433</a>	People's Privacy Act	X	X	X	X	X	IN		X	ALL	X		X	X
					<a href="#">SB 5062</a>	Washington Privacy Act	X	X	X	P	X	X	X~		S/13	X	X	X	X
Washington					<a href="#">HB 1850</a>	Washington Foundational Data Privacy Act													Commission substituted for comprehensive bill *
					<a href="#">SB 5813</a>		X	X	X			X		L	18	X	A	X	X
West Virginia					<a href="#">HB 4454</a>					S		X			16	X		X	
					<a href="#">AB 957</a>		X	X	X	P	X	X	X~		S/13	X	X	X	X
					<a href="#">SB 957</a>		X	X	X	P	X	X	X~		S/13	X	X	X	X
Wisconsin					<a href="#">AB 1050</a>		X		X		X	X		L	16	X		X	
					<a href="#">SB 977</a>		X		X		X	X		L	16	X		X	

						INACTIVE BILLS												
Arizona					<a href="#">HB 2790</a>		X	X	X	X	X		X			X		X
					<a href="#">SB 1864</a>	Florida Privacy Protection Act	X	X	X	P		X	X		S/16	X		X
Florida					<a href="#">HB 9</a>		X	X	X		X	X		L	18	X		X
Georgia					<a href="#">SB 394</a>	Georgia Computer Data Privacy Act	X		X		X	IN		X	ALL	X		X
					<a href="#">HB 2051</a>	Hawaii Consumer Privacy Act	X	X	X	S	X	X	*		16	X	*	X
					<a href="#">SB 2428</a>	Consumer Data Protection Act	X	X	X	P	X	X	X~		S/16	X	X	X
Hawaii					<a href="#">SB 2797</a>	Consumer Data Protection Act	X	X	X	P	X	X	X~		S/16	X	X	X
					<a href="#">HB 2341</a>	Consumer Data Protection Act	X	X	X	P	X	X	X~		S/16	X	X	X
					<a href="#">HB 1261</a>		X	X	X	X		X			16	X		
Indiana					<a href="#">SB 358</a>		X	X	X	P	X	X	X~		S/13	X	X	X
					<a href="#">HF 2506</a>		X		X	P	X	X	X~		13	X		X
Iowa					<a href="#">SF 2208</a>		X	X	X	P	X	X	X~		S/13	X	X	X
					<a href="#">SB 15</a>		X		X		X	X		L	S/18	X	X	X
Kentucky					<a href="#">HB 586</a>		X		X		X	X			13	X		X
Maine					<a href="#">LD 1982</a>	Maine Consumer Privacy Act	X		X		X	X		L	16	X		X
Maryland					<a href="#">SB 11</a>													
					<a href="#">S 46 *</a>	Massachusetts Information Privacy Act	X	X	X	X	X	IN	X	X	ALL	X		X
Massachusetts					<a href="#">H 142 *</a>	Massachusetts Information Privacy Act	X	X	X	X	X	IN	X	X	ALL	X		X
					<a href="#">H 136 *</a>		X	X	X	X	X	X	X~	X		X	A	X

# What Can We Do:



- ▶ Keep abreast of the state laws being proposed with untenable provisions including:
  - ▶ Right to Private Action
  - ▶ Opt-In vs. Opt-Out
- ▶ Oklahoma privacy bill (HB 2969) initially passed the state House and included the nation's first opt-in privacy statute
- ▶ Nonprofits used their voice (specifically ones with a presence in the state)
- ▶ The bill ultimately was not taken up by the state Senate and effectively dies on this year's legislative calendar

# Colorado Privacy Act



- ▶ Takes effect 7/1/23, it does not exempt nonprofits and the partners that do work on their behalf
- ▶ On April 12, AG released email requesting input / comments about what other issues should be addressed in the rulemaking process
- ▶ The covers any company or organization that does business in the state and control or process the data of 25,000 Coloradans
  - ▶ What is unclear is if a nonprofit solicits funds in the state if this is considered “conducting business”
  - ▶ The law allows consumers to correct personal information and have information deleted
  - ▶ It provides for meaningful privacy notice to consumers with details their various rights
- ▶ The time to get involved is now! The TNPA is working to help educate nonprofits and collect information that it can share during this rule making process. The cost of compliance for a patchwork of laws with different tentacles can be high.

# Know the Legal Rules

- ▶ State attorneys general often follow the Federal Trade Commission's (FTC) lead in enforcing state laws on unfairness and deception.
- ▶ Practices that the FTC has identified as factors in reasonable security:
  - Minimizing the collection of personal information;
  - Failure to implement and enforce appropriate password policies;
  - Failure to use encryption to protect consumer information in storage and in transit;
  - Failure to perform due diligence of and oversight of service providers' cybersecurity practices;
  - Failure to provide employees with adequate cybersecurity training;
  - Failure to implement policies and procedures to detect and respond to a breach.

# Know the Legal Rules

- ▶ State Data Security Laws:

Many states require that organizations implement sufficient policies and procedures to maintain reasonable data security

Typically apply based on individuals' residence, not the entity's location

AR, CA, FL, CT, IN, MD, OR, TX, UT & NY are example

- ▶ Data Disposal:

- Approximately 30 states impose legal obligations on organizations to properly dispose of records that contain personal, financial, or health information

# California Consumer Protection Act (CCPA)

*Providing individuals with more control of their privacy*



# California Consumer Privacy Act of 2018 (CCPA)

## What is CCPA/CPRA?

- ▶ The California Consumer Privacy Act of 2018 (CCPA) establishes new consumer privacy rights and expands liability for consumer data breaches.
- ▶ The California Privacy Rights Act ballot initiative passed in November 2020, with the majority of its provisions becoming operative Jan. 1, 2023

Consumers have the right to

- ▶ Learn categories of personal information that businesses collect, sell, or disclose about them.
- ▶ To whom information is sold or disclosed.

# What is the New in CRPA

- ▶ It introduces a new classification of personal information (PI), named sensitive personal information (SPI) that has additional use, disclosure, and opt-out requirements.
- ▶ It requires companies holding high-risk data to conduct annual cybersecurity audits, the results of which must be submitted to the CPPA.
- ▶ It expands on the CCPA's right to opt-out and states that companies must allow consumers the right to opt-out of third-party sharing for advertising purposes.
- ▶ It strengthens consumers' rights by adding the right to delete or correct their personal information. If the said PI has been shared with third parties by the business, the business must notify them of the request to delete/amend as well.
- ▶ It expands on the consumers' right to know provisions in the CCPA.
- ▶ It introduces changes in data governance and transparency, including limitations on storage, data minimization, and contract requirements. Only data that is necessary for the purpose stated by the business must be collected, used, or disclosed. Also, data must be retained only for as long as it is necessary for the said purpose.

# Other Things to Know

Californians are protected in their roles as consumers, employees, patients, tenants, students, parents and children. This includes any information that relates to a particular consumer or household.



- ▶ Note that SP1059 amends the California Data Broker Registration provisions, expanding the definition of "data broker" and requiring data brokers to register with the California Privacy Protection Agency instead of the attorney general. The bill also expands the scope of information data brokers must provide.
- ▶ The CCPA defines personal information as "any information that relates to a particular consumer or household," as well as "inferences drawn from any of the information identified."
- ▶ Since households are covered, data can be protected even if it doesn't relate to a single individual and if it doesn't contain a name.
- ▶ For example: web browsing history and "purchasing tendencies" will be regulated as personal information, even if no names are associated with it.

# New York SHIELD Act

- ▶ On July 25, 2019, New York Governor Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security (SHIELD) Act.
- ▶ The law boosts the protection of consumers' private information, and holds accountable any company that does business within the state.
- ▶ While many states' laws include similar "reasonable" data security requirements, the SHIELD Act takes additional steps by setting forth a detailed series of options for businesses to satisfy this requirement.
- ▶ Although there are federal and state protections of varying strictness already in existence, the New York law will have a broader impact simply due to the size of the state. Here's what you need to know.

# NY Shield Act Takeaways - What is New

- ▶ **It protects a larger set of personal information.** New York's SHIELD law will protect the following information: biometric information resulting from facial recognition software or other means, email addresses and their passwords (as well as security questions and answers), Social Security numbers, driver's license or non-drive ID card numbers and any account number including debit and credit card information with or without security or access codes. This results in more data elements requiring notification if breached.
- ▶ The SHIELD Act also requires businesses that own or license computerized data - which includes Private Information of a resident of New York - to develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the Private Information, including, but not limited to, disposal of data.

# Nuts and Bolts

## How to Comply with the NY Shield Act

- ▶ Designating an employee or employees to coordinate the data security program.
- ▶ Training and managing employees in the security program practices and procedures.
- ▶ Assessing internal and external risks and implementing controls to reduce those risks.
- ▶ Vetting service providers and binding them contractually to safeguard private information.
- ▶ Securely destroying private information within a reasonable amount of time after it is no longer needed for business purposes.

# STAY UP TO DATE

- ▶ Cybersecurity risk management is not a “one-time” effort
- ▶ Legal standards and security threats are constantly evolving
- ▶ Consider periodic review and reassessment, particularly following a breach

# The Future of Privacy

## *PRIVACY IS HERE TO STAY*

- ▶ At least 38 states introduced more than 160 consumer privacy related bills in 2021 (compared to 30 states in 2020 and 25 in 2019).
- ▶ Comprehensive privacy legislation was the most common type of bill, introduced in at least 25 states.
- ▶ Legislation aimed at information brokers was introduced in 11 states. California, Nevada and Vermont had previously enacted laws, and Nevada in 2021 enacted legislation expanding its law, but no other bills passed.

# Legislation with Focus on Data Brokers

- ▶ Alaska (AK SB 116/AZ HB 2790) Establishes the Consumer Data Privacy Act, establishes data broker registration requirements, makes a violation of the Act an unfair or deceptive trade practice; Relates to personal data, relates to processing, relates to security standards.
- ▶ Delaware (DE HB 262) Provide consumers with information about how their personal information is being used by data brokers, requires registration and the answer of questions regarding their use of personal information that would be published online to inform consumers.
- ▶ Maine (MA HB 699 & ME LR 1604) Creates the Maine Data Collection Protection Act, which prohibits data collectors from collecting and aggregating, selling or using specific types of public documents or information from those documents for the purpose of determining a consumer's eligibility for consumer credit, employment or residential housing; Creates a data broker registry and improve consumer protections.
- ▶ NY (NY AB 680) Enacts the NY privacy act to require companies to disclose their methods of de-identifying personal information, to place special safeguards around data sharing and to allow consumers to obtain the names of all entities with whom their information is shared, creates a special account to fund a new office of privacy and data protection.

# What We Want

- ▶ National policy that provides preemption of state laws, with a uniform set of standards & guidelines
- ▶ Oversight of the legislation that lives with the federal court (not state)
- ▶ Include Opt-out vs. Opt-in language
- ▶ Does not allow for any Private Right of Action
  - ▶ Historically PRA has led to class action lawsuits that even if they are unfounded or frivolous can create a significant liability concerns

# Wake-up Call

## Organizations experiencing loss of PII grows each year

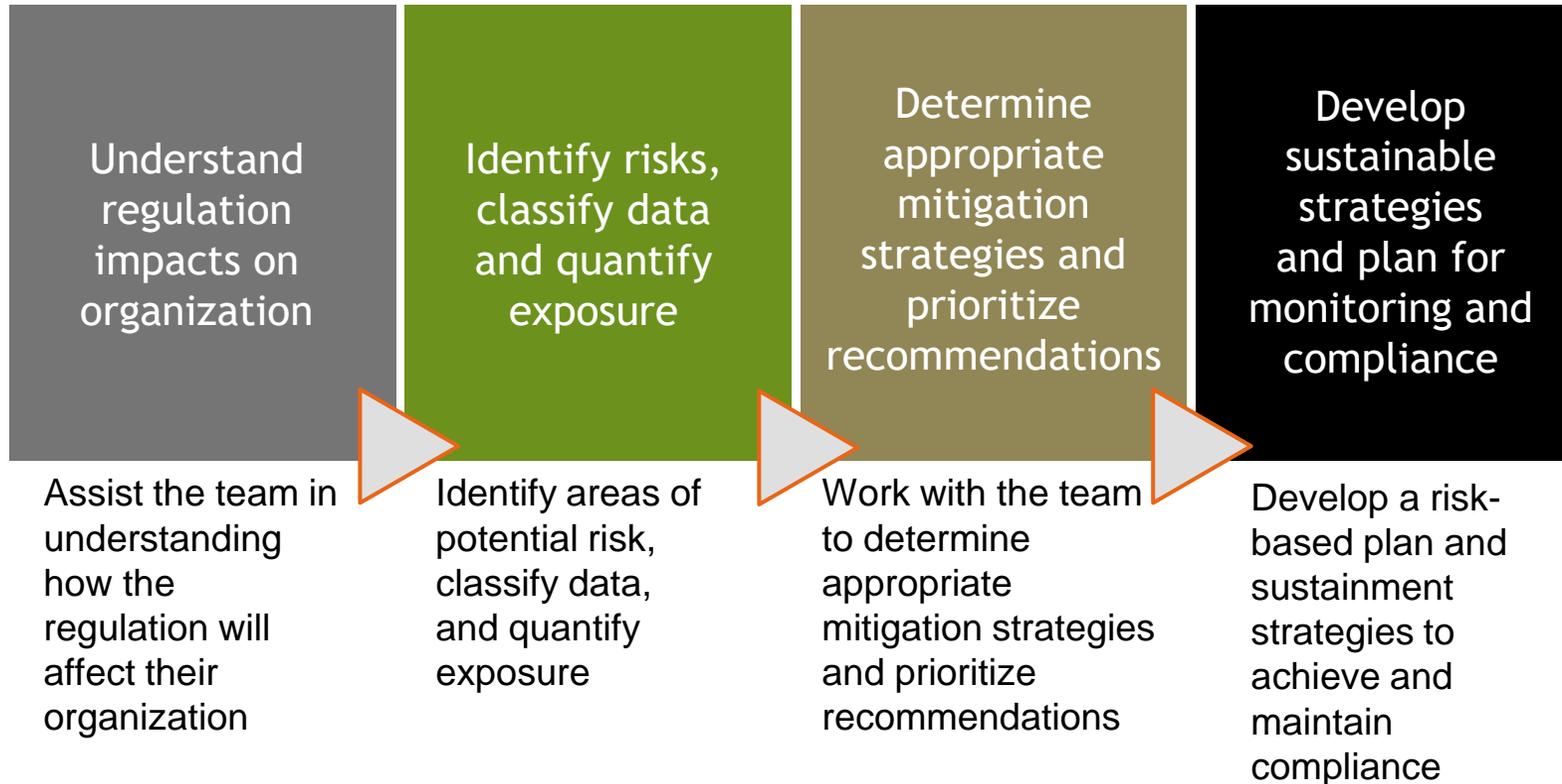
- ▶ Data breaches are the leading threat in today's digital world, with a new cyberattack occurring approximately every 39 seconds.
- ▶ Cost of a Data Breach: Many factors contribute to total costs: Breach response efforts delivering notices, credit monitoring, legal costs, etc. - Reputational costs, customer and employee goodwill, media scrutiny - litigation and or regulatory defense
- ▶ The financial costs of managing a data breach are well documented and growing, with a recent study estimating the cost of a data breach in 2021 was \$ 4.24 million
- ▶ This is a 10% rise from the average cost in 2019.

# Why Protecting Data (“PII”) is Important

- ▶ Data is a valuable organization asset, like any other
- ▶ Data is at a higher risk of theft or misuse than ever before
- ▶ Loss of data can have long-lasting consequences
  - ▶ Reputational harm
  - ▶ Loss of donor trust
  - ▶ Financial penalties and costs
  - ▶ Legal liability
- ▶ Organizations have obligations to protect data
  - ▶ Laws, regulations, guidelines
  - ▶ Contracts with third parties
  - ▶ Privacy policies

# Privacy Readiness

Assessment to set the bounds for privacy compliance





# First Step

## Website Privacy Policy

### Best practices

- ▶ Clear and concise
- ▶ Comprehensive
- ▶ Comprehensible
- ▶ Current (revisit each year)

### Key Elements

- ▶ Delineate the PII and Non-PII that is Collected
- ▶ Disclose How the Data will be Shared
- ▶ Address Data Collection from Minors
- ▶ Ensure that you Reserve the Right to Make Changes
- ▶ Address Applicable Laws (GDPR)

**Don't Forget Your Terms of Use!**

# Mitigate Cybersecurity Risks

## *Focus on Vendors*

- ▶ Organizations are increasingly relying on third parties to provide critical services, and to host PII of their donors and employees.
- ▶ Unfortunately, these vendor contracts are typically extremely one sided in favor of the vendor.
- ▶ Review contracts with vendors that collect, process or hold your PII
  - ▶ Privacy and Security
  - ▶ Limitation of Liability
  - ▶ Indemnifications
  - ▶ Breach Notification

# Mitigate Cybersecurity Risks

## Adopt a Data Retention and Deletion Plans

### Get Organized

- ▶ First step in any retention policy process is to organize the data you already have.

### Get Informed

- ▶ State, federal, and tax laws may vary with respect to what data and communication you are expected to retain and for how long. You will certainly want to consult legal counsel at this point.

### Get Backed Up

- ▶ No policy in the world can help you if you don't implement physical methods of ensuring that data is protected until you decide to take action on it.

### Get Destructive

- ▶ Backing up takes care of the stuff you need to retain indefinitely; you need to have equally robust procedures for destroying data that you decide not to retain

## And Prepare for the Worst...

### *Implement Data Retention and Destruction Policy*

An incident response plan is a document that outlines an organization's procedures, steps, and responsibilities should in incident such a a data breach occurs.

Having an incident response plan is actually required by the New York SHIELD Act - and is a "best practice in your cyber-hygiene regimen.

Most states have implemented a data breach notification statute; federal legislation is being considered

The requirements for notification can vary widely by state; many states require notice to state authorities as well as individuals

And not all security incidents require notification

- Where a "breach" did not occur
- Where the information involved was not "personal information" - Where there is no risk of harm to affected individuals

# Mitigate Cybersecurity Risks

## *Cybersecurity Insurance*

- ▶ Identify your unique risks
- ▶ Match your insurance to your company's risks
- ▶ Beware of exclusions
- ▶ Consider coverage for acts by third parties
- ▶ Negotiate for an early retroactive date
- ▶ Understand the “triggers”
- ▶ Evaluate coverage for data restoration costs
- ▶ Consider coverage for loss of information on unencrypted devices
- ▶ Consider coverage for regulatory actions

# Elementary Do's / Don'ts

## DO

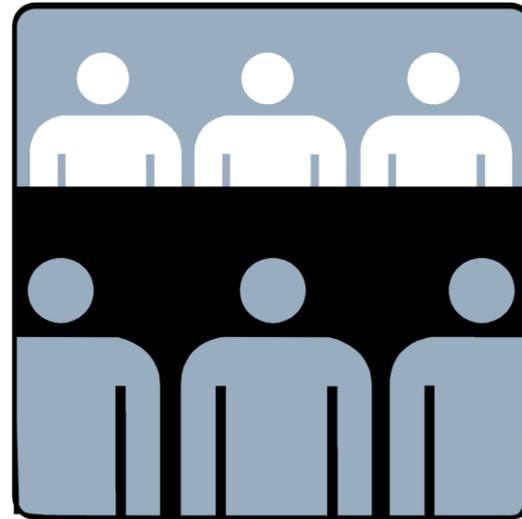
- ▶ Set up secure transmission methods (MFP, SFTP) to transmit data
- ▶ Ensure your clients have clear privacy policies that cover them for exchanging or sharing data
- ▶ Understand Consumers' Rights to Access, Delete & Opt-Out
- ▶ Establish Organizational Best Practices for Responding to Consumer/Donor requests (regardless of nonprofit exception)
- ▶ For nonprofits - Build trust with your donors by providing transparency

# Elementary Do's / Don'ts

## Don't

- ▶ Send consumer/donor information via email to your data partners
- ▶ Don't accept consumer/donor information via email from your clients

# Q & A



About Our Firm

Attorneys

Practice Areas

Fundraising Compliance

Insights

Contact



### About Our Firm

As an experienced advisor to nonprofits and social enterprises, we help our clients optimize their social impact.

[Read More](#)



### Attorneys

We are a team of dedicated attorneys driven by a shared passion: helping to make the world a better place.

[Read More](#)



### Practice Areas

Our firm addresses legal issues for nonprofits and social enterprises in all phases of the business life cycle.

[Read More](#)



### Fundraising Compliance

We handle registrations for hundreds of nonprofits, fundraisers, and commercial co-venturers to insure they are in compliance.

[Read More](#)

[www.perlmanandperlman.com](http://www.perlmanandperlman.com)

[jon@perlmanandperlman.com](mailto:jon@perlmanandperlman.com)



# LIST BAZAAR

The Legend returns...

THANK YOU!