How Nonprofits can Protect their Data and Reputation in the New Era of Data Privacy

The United States is bracing for a new wave of privacy laws and, whether you're a Fortune 500 company or a small nonprofit, you will be impacted. As an example, on Nov. 3, 2020, California voters passed the California Privacy Rights Act (CPRA), making it clear, once again, that American consumers are seeking enhanced privacy laws to protect their personal information. The CPRA amended key portions of the 2018 California Consumer Privacy Act (CCPA) and will take effect in January 2023.

Consumer information privacy regulation laws are gaining traction across the country and will continue to become more prevalent and robust as more states adopt new legislation. There are currently several CCPA copycat laws being considered in other states including:

- Nebraska Consumer Data Privacy Act (Legislative Bill 746)
- Virginia Privacy Act (HB 473)
- New York Privacy Act (Senate Bill 5642/A)

Although nonprofit organizations are typically exempt from consumer privacy regulation laws like the CPRA, their members, donors and staff still expect to have their personal information secured and protected. A nonprofit that experiences a ransomware attack or a data breach can still be impacted by data breach notification laws in addition to bad publicity and a loss of trust in their services. Nonprofits need to successfully know, protect and govern their data to create a data privacy protection plan.

KNOW YOUR DATA

Most nonprofit organizations entrust their data storage to third-party hosting providers and applications to minimize their in-house IT footprint. This may help cut costs, but it makes it challenging for nonprofits to answer key data privacy questions such as:

- Who has access to our data?
- Where does our data go (e.g., other vendors)?
- How long is our data retained?
- When does data get deleted?

When engaging third parties, nonprofits need to evaluate vendor contracts to ensure that they contain necessary data protection clauses regarding data storage, data management, data retention and destruction.

Vendor contracts should be evaluated to:

- Ensure that they are current and can withstand the scrutiny of a regulator
- Evaluate risk thresholds to ensure that the organization is protected if the vendor experiences a data breach
- Review current insurance policies, such as cyber liability insurance, to determine whether ample protections are in place

PROTECT YOUR DATA

Personal data, such as information on donors, members and recipients of services, is the lifeblood of a nonprofit, and protecting it should be a top priority. There has been a recent uptick in business email compromise attacks that have organizations of all sizes reconsidering their data protection tactics.

To create a comprehensive data protection program, an organization should consider:

- Data classification schemas to understand where personal data resides and who has access to it
- Incident response plans to ensure that there is a mechanism to respond if (and when) an incident or a breach occurs
- Administrative and technical controls to ensure they are current and that patches are implemented at appropriate times
- User policies and how data should be handled and monitored

GOVERN YOUR DATA

Data governance helps an organization define who can do what with the data it stores by creating a set of processes, roles, policies and metrics to manage data. Data governance programs can increase the quality of data, eliminate redundancy and allow the nonprofit to make better decisions faster.

Data governance programs should include:

- An executive-level champion that secures resources
- A charter that outlines the purpose of the program and how it will be managed
- A cross-functional committee that is assigned roles and responsibilities to deliver the program
- A program manager that can help move tasks and initiatives forward
- Funding to support initiatives

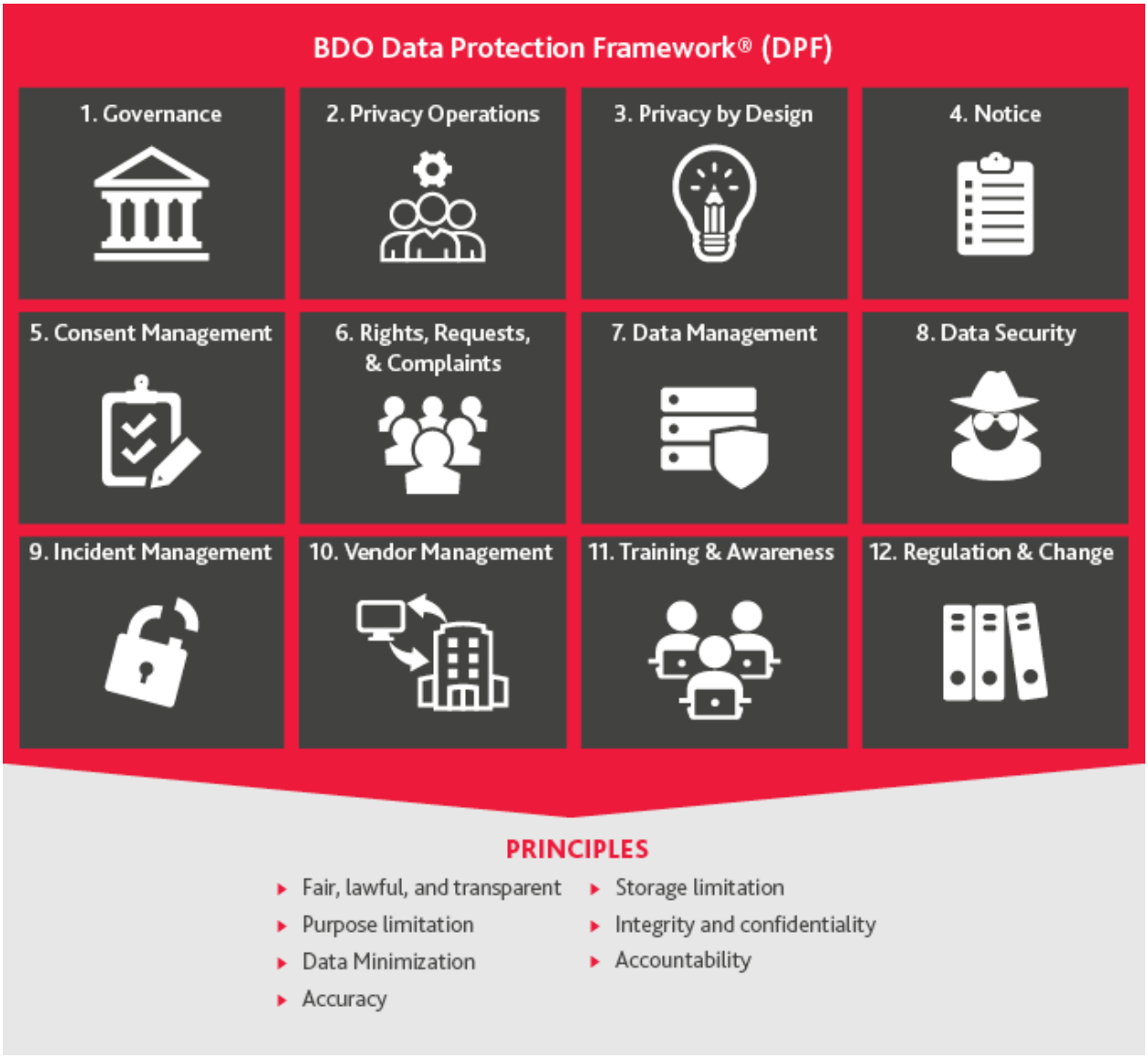
Steps to creating a data governance program include:

1. Identifying the locations of personal data
2. Determining which databases or sources contain the most valuable personal data (highest risk data)
3. Evaluating the accuracy, redundancy and relevance of these data sets
4. Remediating data sources that are outdated, redundant or provide no value to the organization or its stakeholders
5. Determining if appropriate data protection administrative and technical safeguards are in place
6. Developing a go-forward plan that allows for routine evaluations of the data that reduces the amount of unnecessary data that is retained for periods that are reasonable

Developing a data privacy protection plan can seem like a daunting task, but nonprofits that know, protect and govern their data are already on their way to meeting the demands of future data privacy laws.

Build a Holistic Data Protection Program by using a Trusted Framework

BDO Digital has developed a data protection framework to help nonprofits build strong privacy programs that allow organizations to meet the needs of stakeholders, members and customers.


BDO Data Protection Framework® (DPF)
1. Governance
2. Privacy Operations
3. Privacy by Design
4. Notice
5. Consent Management
6. Rights, Requests, & Complaints
7. Data Management
8. Data Security
9. Incident Management
10. Vendor Management
11. Training & Awareness
12. Regulation & Change
PRINCIPLES
Fair, lawful, and transparent
Purpose limitation
Data Minimization
Accuracy
Storage limitation
Integrity and confidentiality
Accountability