Practices, Policies and Procedures to Minimize Cyber Security Risk and Comply with Data-Privacy Regulations

The data you collect about donors, volunteers, and beneficiaries is among a nonprofit organization's most valuable assets, and its management and protection should be viewed as mission-critical stewardship. Each year the stakes get higher as increasingly sophisticated "cyber-attacks" result in larger and more costly cyber incidents, and new regulatory schemes impose a plethora of new obligations, and require new processes and practices. This checklist is designed to help organizations and their for-profit partners assess risk - and implement best practices to substantially and meaningfully mitigate those risks – and understand and evaluate their compliance with some of the recently and soon-to-be enacted regulatory schemes.

☐ **Data Privacy Audit** – Considering the increasing prevalence of data breaches, all organizations should conduct a data-privacy audit. This audit documents how data is being collected, stored, protected and shared. Understanding these "data flows" is the first step in minimizing data-incident risk. Key audit themes include:

- Cataloging the data being collected
- Identifying who (including third party vendors) has access to the data
- Assessing how the data is protected, processed and deleted

☐ **MSA Review** – *For Profit Service Providers*: Your standard customer agreement is a crucial document that establishes key legal terms and is critical in managing the overall risk of the organization. Key provisions that your MSA should include:

- Exclusion of special/punitive damages; limits on direct damages
- Appropriate and customary warranty disclaimers
- IP ownership and licensing of "background" work product
- Up-to-date professional fundraising/consulting disclaimers/terms
- Compliance with applicable regulatory privacy schemes

☐ **Third Party Vendor Review** – *Nonprofit Organizations*: As organizations are increasingly relying on third party vendors to store, process and manage data – and as these vendors are often the source of data incidents - negotiating contractual terms have never been more important to protect your organization and minimize financial risk. Key terms to include in all contracts with vendors who have access to data include:

- Breach Notification/Credit Monitoring
- Appropriate carveouts to any limitations on liability
- Transition Services
- Specific provisions related to data security and privacy
- Appropriate insurance requirements and terms

☐ **Cyber Security Insurance** – Given the potential costs associated with a data breach, cyber security insurance is a necessity. Policies can widely differ, and all policy terms should be reviewed. Key coverage provisions include:

- Data breach liability
- Data loss coverage
- Forensic investigation indemnity
- Notification costs coverage
- Public relations expenses/crisis management/legal defense
- Settlements, damages and judgments coverage related to the breach.
- Cost related to responding to regulatory inquiries, regulatory fines and penalties

☐ **Website Privacy/Terms of Use Policy Review –** Every website should have a posted privacy policy and term of use. Privacy policy and terms of use are key online agreements that should be reviewed annually to ensure compliance with legal requirements and best practices.

☐ **Data Retention and Destruction Policy** – The more data you retain, the more you risk should a breach occur. Implementing a data retention and destruction policy will help to mitigate such risk.

☐ **Incident Response Plan –** Documenting and preparing for a security breach, cyber-attack, or other incident has proven to be a critical factor in limiting damage, reducing recovery time and containing costs. If your organization does not have a policy, one should be created and adopted ASAP.

☐ **New York SHIIELD Act** - This Act applies to both nonprofit and for profit businesses that collect "private information" on NY residents, regardless of whether the business conducts business in the state of NY. Requirements include:

- Designation and training of employees to coordinate cybersecurity compliance
- The use of third-party service providers capable of maintaining appropriate

Presented By: Jon Dartley, Esq.,
Perlman & Perlman, LLP
212.889.0575 ext. 224
jon@perlmanandperlman.com

cybersecurity practices, with certain contractual safeguards

- Risk assessment of your organization's current cybersecurity program
- Processes to safely, securely and permanently dispose of data within a reasonable amount of time after it is no longer needed for business purposes

☐ **The California Consumer Privacy Act (CCPA)** - This Act goes into effect January 1, 2020. Considered one of the strictest privacy laws in the United States, CCPA provides California residents with the ability to control how businesses process their personal information. While CCPA primarily applies to for-profit organizations meeting certain threshold parameters, there are some instances in which it will apply to nonprofit organizations. To comply, organizations will have to adopt a variety of new measures, including:

- Draft and post a comprehensive privacy notice (see addendum 1 for specific elements that must be addressed)
- Create straightforward process to opt-out of the sale (defined as any sharing in which there is some value provided in return, including exchange) of personal information
- Have processes and procedures to delete all personal information at the request of the consumer
- For nonprofit organizations – ensure written confirmation and related contractual terms that your for-profit partners/vendors are compliant

☐ **General Data Protection Regulation ("GDPR")** - GDPR applies to most organizations transacting in the EU, imposes a broad range of new obligations related to the collection and processing of personal information, and comes with steep penalties for non-compliance. To comply, organizations should first determine whether they are a "data processor" or "data controller", and then will need to adopt a variety of new measures, including:

- Draft and post a comprehensive GDPR Privacy Notice (see addendum 2 for specific elements that must be addressed)
- Specific internal policies and practices related to data processing
- In regard to for-profit organizations, create "customer GDPR addendums"
- In regard to nonprofits, ensure you have GDPR amendments with all relevant vendors

Presented By: Jon Dartley, Esq.,
Perlman & Perlman, LLP
212.889.0575 ext. 224
jon@perlmanandperlman.com

Addendum 1 – CCPA Privacy Policy Requirements

CCPA requires the operator of a commercial website or online service that collects personally identifiable information about a California consumer to post a privacy notice. A CCPA compliant privacy notice should contain the following elements:

- Description of the new rights afforded California residents
- Description of the methods for submitting a personal information or erasure request
- A link to an opt-out page on the website
- A list of all the categories of personal information that have been collected in the past 12 months
- The sources of each category of personal information
- All of the purposes for using each category of collected information
- A list of the categories of personal information sold in the past 12 months
- A list of the categories of personal information disclosed for a business purpose in the past 12 months
- Description how the website responds to do-not-track signals from a user's browser
- Disclosure of whether it permits third parties to collect information about website visitors' online activities over time and across other websites

Presented By: Jon Dartley, Esq.,
Perlman & Perlman, LLP
212.889.0575 ext. 224
jon@perlmanandperlman.com

Addendum 2 – GDPR Privacy Policy Requirements

Transparency and informing the public about how their information is being used are two basic goals of the GDPR. A privacy notice is a public document from an organization that explains how that organization processes personal information and how it applies data protection principles. If you are collecting information directly from someone residing in the European Economic Area, you have to provide them with your privacy notice at the moment you collect such information. A GDPR compliant privacy notice should contain the following elements:

- The identity and contact details of the organization, its representative, and its Data Protection Officer (if applicable)
- The purpose for the organization to process an individual's personal data and its legal basis
- The legitimate interests of the organization (or third party, where applicable)
- Any recipient or categories of recipients of an individual's data
- The details regarding any transfer of personal data to a third country and the safeguards taken
- The retention period or criteria used to determine the retention period of the data
- The 8 rights they have under the GDPR
- The right to lodge a complaint with a supervisory authority
- The existence of an automated decision-making system, including profiling, and information about how this system has been set up, the significance, and the consequences (if applicable)

DISCLAIMER:
These materials were prepared for informational purposes only. The information contained herein is general in nature and may not have application to particular factual or legal circumstances. These materials do not constitute legal advice or opinions and should not be relied upon as such. Transmission of the information is not intended to create, and receipt does not constitute, an attorney-client relationship. Recipients of this information should not act upon any information in this article without seeking professional counsel.

Presented By: Jon Dartley, Esq.,
Perlman & Perlman, LLP
212.889.0575 ext. 224
jon@perlmanandperlman.com