This article presents general guidelines for Georgia nonprofit organizations as of the date written and should not be construed as legal advice. Always consult an attorney to address your particular situation.

Privacy Rule Basics in the Face of a Privacy Storm

By Dawn Kimmich, Assistant General Counsel, Delta Air Lines

In everyday media, privacy is the buzz word. Organizations have been nervously busy for some time understanding which privacy rules apply to their businesses. Often more than one regulation applies. In 2018, the European Union adopted the General Data Protection Regulation (GDPR), data privacy regulations which are influencing data privacy rules and practices in the United States and internationally. California also has a new privacy law to consider. Here are some practical privacy compliance program considerations for smaller organizations:

Understand PII. Nonprofit organizations should start with understanding which personal data they obtain from clients, program participants, vendors, donors, and employees. Personally identifiable information (PII) is defined quite broadly, under the GDPR and other existing regulations. PII includes name, address, date of birth, sex, race, marital status, age, nationality, religion, birth place, passport and driver's license numbers, telephone numbers, email addresses, IP addresses, credit card and bank account numbers, and credit scores. The list is longer and broader than that. Some data is considered highly sensitive, such as health data or criminal history, and this data bears a higher burden of care.

Reasons for collecting the data? Once the organization knows which data it has, it needs to know why. If the organization sells a product online, it might collect customer shipping information so as to complete the transaction. If it's providing a service, there is likely even more PII in play.

Some organizations go beyond the transaction, and retain PII for future marketing, or product development. There can be a higher burden (consent requirement) if the plan is to market using PII.

In more extreme cases, some organizations collect and sell data to a 3rd party, and here, the burden really grows. If reasonable individuals would not expect that their data would be used in this or that manner, this is a red flag. People generally complain, even more so today, when they feel that their privacy is violated. Spam emails now fall into the scope of privacy protections. In more extreme examples, customers complain to privacy regulators about companies (particularly in the European Union or EU), and the organization then faces inquiry, regulatory audits, and fines. For example, Google was recently fined over $50 million in the EU because of a data breach.

Minimization. Minimization is about collecting only the PII that an organization truly needs to run the business, and not more. For example, an organization should collect only the PII necessary to complete a transaction (provide the services, make the product, ship the goods, or bill and collect payment). As an example of collecting more PII than necessary, if the organization operates a food bank that distributes food to clients, it probably does not need to know blood type or religion to perform its service. Similarly,

if the organization is selling a product, it does not need age or marital status, but rather only a shipping address and credit card. A good first privacy mitigation step is to not ask clients for unnecessary PII.

Access. Many conscientious organizations limit employee access to personally identifiable information to a need to know basis. Employees in Human Resources do not have access to customer databases. Sales employees do not have access to employee databases. Additional controls exist to gain access to highly sensitive personally identifiable information (e.g. medical information). To reduce the risk of a data breach, organizations need to understand who has access to the most sensitive PII, or any PII, and revoke unnecessary access credentials.

Privacy Policy. Many organizations have aPrivacy Policy. This policy provides notice of which PII the organization collects, and for which purposes. It provides contact details for privacy questions. Employees and clients need not give consent to the Privacy Policy, but they often receive notification of it, particularly at the moment of collection (e.g. when applying for services, providing payment details, or completing an employment application). Many organizations post their Privacy Policy on the home page of the website where it is easy to find. Some also issue client and employee communications about the new Privacy Policy.

Having a Business Purpose or Consent. Under the recently adopted data privacy regulations in the European Union (EU), organizations need a valid basis for collecting every type of PII.

One valid basis is a legitimate business reason. For example, an organization selling a product online legitimately needs a physical address, and a recipient's name, to send the final product and complete the transaction.

Consent is another legal basis for collecting PII under these regulations. However, getting proper consent is not as easy as it sounds. To rely on consent as the basis for collecting PII, the consent must be explicit, express, captured, and documented. And, to further complicate the effort, under EU rules, an individual can revoke consent at any time. People can change their minds. This means that an organization needs to database from whom it has consent, how and when they got it, and also be able to change course (e.g. stop marketing to an individual) if consent is revoked. In practical terms, an organization needs consent if it plans to collect or keep PII for marketing.

Not all consents are equal. We all recognize the pre-checked box which signs us up to receive all manner of advertisements and newsletters. The pre-checked box is called opt-out consent, because the individual has to take an action to opt out use of their PII, i.e. receiving marketing. The EU requires opt-in consent, namely that the box is **not** pre-checked, and the individual must take action if she wants those emails.

Limited Retention. Existing privacy rules require organizations to keep data only for as long as is necessary to achieve the purposes for which the data was collected. Certainly, organizations can keep data to finalize transactions or until reporting on grants or donations is completed. Keeping data beyond such typical periods can lead to headaches if a breach occurs. Some organizations never purge once they figure out where and how to store data, but this is an outdated practice. Keeping less data means exposing less data.

Additional Protections of PII. Organizations in the regular practice of sending large amounts of particularly sensitive PII use various methods to further protect PII. These include encryption at rest (within the storage system); encryption during transfer (when sending information); encrypted thumb drives (readily available); automatic email purges; password expiration; encrypted emails; limiting recipients; and password protected documents.

Cookies. Organizations which communicate in the market via the internet, and who use cookies on those sites, should give their clients notice of those cookies on the website. These cookie banners are common now, and generally require the browser to consent to cookies through at least one click.

Oversight, Training, and Communications. Regardless of size, it is a best practice for organizations generally to assign privacy as a responsibility to at least one person. If the organization has someone with IT knowledge, that would be the logical person to take on this responsibility. If not, the Executive Director may need to do so, with the ability to consult with IT support as necessary. This gives a face (and an advisor) of privacy to all employees.

Employees need training to avoid careless errors such as losing or leaving papers with PII in view, losing a USB drive, sharing passwords, sending personal data to the wrong recipients, or posting it to those who do not need to know. Many vendors sell generic privacy training, but PowerPoint slides may also suffice for training. Leaders may want to send memos to all employees, and host privacy awareness days, to reinforce the organization's privacy stance. Training and communications generally recur, as this reminds employees of their obligations under the Privacy Policy.

Conclusion. Nonprofit organizations should collect only that PII needed, should limit access to the PII that is collected, should retain the PII only for so long as needed, and should adopt a Privacy Policy and implement communication and training so that employees understand the rules and restrictions related to collecting and protecting PII. By implementing these steps to protect the private information of clients, program participants, vendors, donors, and employees, the organization can minimize the risk of a data breach or the unauthorized disclosure of PII.