Beginner's Guide to Data Privacy Laws

By Lindsey Whinnery, Partner

It's no secret that data security and data privacy have now entered the legal realm. News headlines continue to alert readers to data breaches, but now they are also peppered with updates on new laws appearing on the local, national, and international scene.

These laws are long overdue, and every organization should be aware of what they encompass.

European and U.S. Laws

The United States currently lacks federal legislation related to data privacy and security. Many states have enacted some form of law related to this topic, but most are highly ineffective in the current cyber climate.

The European Union (EU) propelled this subject into mainstream news with the passage of the General Data Protection Regulation (GDPR), which went into effect in May 2018.

These laws are long overdue, and every organization should be aware of what they encompass.

The advent of the GDPR, coupled with what seems like daily data breaches, stirred the U.S. government to begin developing privacy laws, and state governments to dust off their old laws and give them a much-needed facelift.

In December 2018, the U.S. Senate introduced the Data Care Act of 2018, which is an attempt to enforce privacy and security of data on a federal level. Organizations and security professionals are actively monitoring this bill along with other new laws and anxiously waiting to see which will be enforced and how organizations will be impacted.

Compliance Considerations

The GDPR caused quite a commotion when it went into effect. The new regulation is extremely thorough and overreaching. It's also packed with heavy consequences for non-compliance, which the media focused on.

In summary, the GDPR grants many rights to EU citizens, who can exercise these rights even if the organization with their data is not located in the EU. The GDPR also includes requirements for reasonable security measures and stringent breach notification procedures. On the other hand, here in the U.S. many of the revised state laws include a decreased scope of coverage. These laws primarily focus on three principles: data destruction, a general statement on data security, and breach notification. The specifics on breach notification vary slightly. A handful of state laws include a wider scope of coverage and somewhat resemble the GDPR.

Compliance with the new laws can be daunting. If full compliance is not feasible, the next best approach is to prioritize and focus on smaller objectives. Think of it as a marathon. If you don't currently run, you probably wouldn't start by training for a marathon. A 5k would be a more reasonable goal. That's how you can treat data privacy compliance. Take on the five smaller goals below and once you've accomplished them, you'll be well on your way to compliance. Anything is better than sitting on the couch.

So lace up those shoes and let's get started!

1. Assign responsibility.

The first step to compliance is to designate a Data Security Officer. Depending on the size of your organization, this could be an entirely new role or added to the responsibilities of your Information Security Officer, a member of your IT department, or someone outside the IT department. This doesn't necessarily need to be the individual performing the actions, just someone responsible for ensuring that all elements of the law are being implemented.

Due to the critical nature of the Data Security Officer role, it is best for it to be independent of the IT department to ensure it receives the prioritization it deserves. The

primary role of the IT department is to ensure IT systems are running smoothly, and data security and privacy often fall to the wayside among the daily demands of those tasks.

2. Assess your data risk.

A risk assessment is one of the more critical steps in developing a data security and privacy program. Without a risk assessment, you lack the roadmap to logically address all the threats to your data assets.

The first step is to identify each system or application that contains personal identifying information (PII). Each law defines PII differently, so it is important for your organization to define PII using a collection of applicable laws.

Once all PII has been identified, document the security safeguards you have in place to reduce the risk of a data breach. Examples of protection can include:

- Encryption of data at rest and in transit
- Password parameters
- Account lockout settings
- Multi-factor authentication
- Patch management procedures
- Anti-malware management

If any residual risk remains after those controls have been considered, apply additional safeguards to reduce the risk to a level within your risk appetite.

Finally, identify the geographical areas of PII that your organization houses. The location of the data could affect the steps that must be taken upon a potential or realized breach.

3. Implement controls to protect your data.

After completing the risk assessment, make sure all security controls or safeguards that you have defined in your risk assessment are fully implemented and operating effectively. This is an ideal time to conduct an internal IT audit of controls or engage external expertise to perform an independent audit of IT controls. An internal or external audit will often identify weaknesses in the risk assessment and can pinpoint missing controls that should be implemented to satisfy the legal requirement of *reasonably securing data*.

4. Update your Incident Response Plan.

Incident response procedures are a primary component of the new data laws. Specific notification requirements vary among the laws, but all require certain timeframes, notification methods, and recipients of the notifications. Recipients range from the victims themselves to other parties including, but not limited to, state attorney generals, supervisory authorities (under the GDPR), and credit reporting agencies.

It is crucial to list these differences in your plan, and the accompanying parameters for when notification would be required. With timeframe requirements ranging from 72 hours to well over 60 days, the contact information and responsibility for notification should be clearly assigned in your Incident Response Plan. It is also important to pay attention to the disclaimers in the law, as several include an exception to the timeframe parameter if the security incident is part of an ongoing investigation.

5. Establish front-line procedures.

A handful of these laws (including the GDPR and the California laws) grant new rights to citizens. Some of these include rights to:

- Access their data
- Rectify their data
- Have their data erased
- Receive their data and transmit it to another controller (data portability)
- Opt-out of automated decision-making systems
- Opt-out of data being sold or shared

It's likely that your front-line staff will initially receive these sorts of requests. It's imperative for them to be familiar with response procedures since the time clock on these requests starts the moment your organization receives them. You will also want to ensure that your generic support email addresses and front-line email accounts are actively checked.

Furthermore, you should develop procedures for handling and processing each of these requests. Failure to respond adequately could result in civil litigation, which is a higher likelihood for small to medium-sized organizations than the GDPR non-compliance fines.

Best Practice

These laws will evolve, and we will continue to see international, national, and state laws affect organizations that would usually fall outside of their physical borders and jurisdiction.

Rather than ignoring these new laws, following these initial five steps will position your organization for

Without a risk assessment, you lack the roadmap to logically address all the threats to your data assets.

compliance while reducing your risk of a data breach. Even if you are unsure whether you "have" to comply, you should consider following these steps to help protect your organization and your constituents.

This article was originally published in The Nonprofit Times.

About the Author

Lindsey Whinnery, Partner
CapinTech
lwhinnery@capincrouse.com
o 505.50.CAPIN ext. 2003

Lindsey has over 15 years of experience in information technology and information security. Lindsey provides review and consulting services with an emphasis on nonprofit organizations, higher education, financial institutions, and healthcare facilities. She stays current on changing threats, government regulations, and various organizations' security frameworks to design audit work programs and better assist clients in implementing appropriate controls to protect against cybersecurity threats.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.