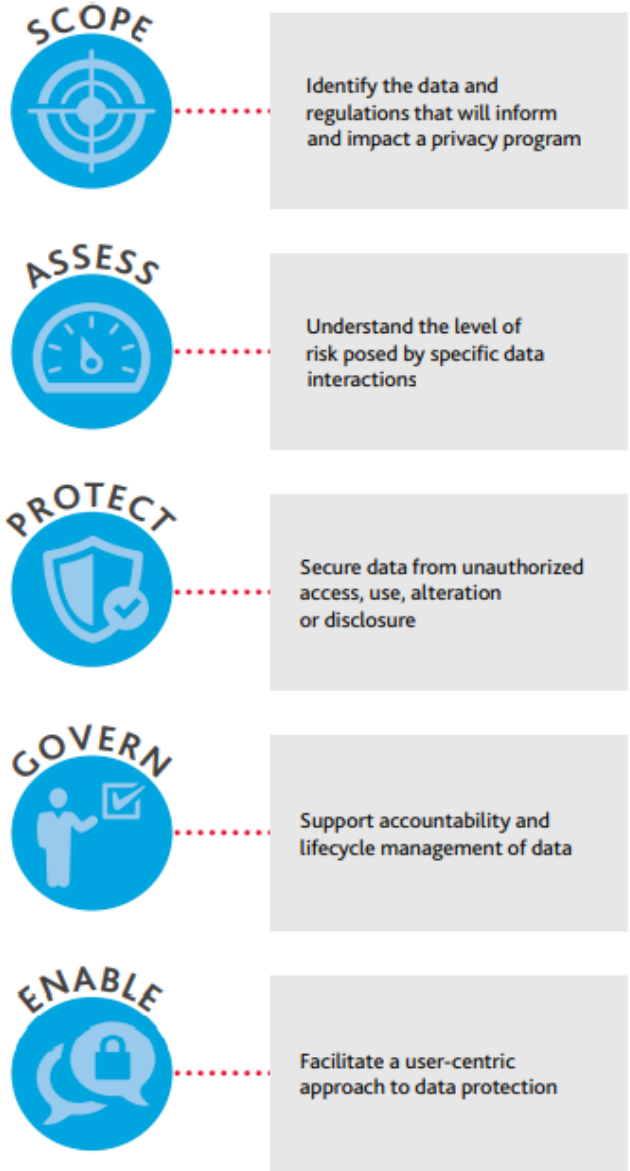
Kral Ussery
Certified Public Accountants
Advisors - Litigation Support - Internal Audit

TX Office: (817) 416-6842
NV Office: (702) 565-2727

Oct 25, 2022

Data Privacy and Governance Checklist for the Board

This checklist outlines the basics for understanding your organization's current data protection posture regarding the handling of personal and sensitive data. Leverage the following questions and responsibilities to enhance your organization's privacy practices and reduce regulatory risk.



SCOPE

APPLICABLE REGULATIONS	DATA MAPS	DATA SUBJECTS
Understand the data privacy regulations that apply to your organization, either as a result of the data you collect and use, or the jurisdictions in which you operate. □ **Does your organization need to be HIPAA compliant? How about GDPR? Maybe CCPA, CPRA, or the Virginia CDPA?**	Understand the different types of data your organization interacts with, where it comes from, and to whom and to where it is traveling. □ **Does your organization maintain data maps or data flow diagrams to track data flowing into, through and out of the organization?**	Be aware of individuals from whom your organization is collecting data. Understand the different laws, rights and protections associated with data from those individuals. □ **Does your organization understand how privacy rights differ among residents of different countries, consumers/customers and your own employees?**

ASSESS

RISK ANALYSIS	IMPACT ASSESSMENTS	RISK MITIGATION
Conduct regular risk assessments to understand the impact of starting a new project, standing up a new information system, setting up operations in a new country or onboarding a new service provider. Identify controls needed to mitigate these risks. □ **Is your new web application compliant with relevant data protection regulations covering the information it is collecting and the locations of the users?**	Perform Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs) for new initiatives, operations, technology implementations and third-party relationships to identify potential privacy risks and measure the performance of mitigating controls. □ **Is your new technology compliant with your data privacy standards?**	Once identified, apply physical and technical safeguards and controls to reduce the data privacy risk associated with your organization's use of data. □ **How much security and privacy risk is your organization prepared to accept, and where are you exceeding that risk level?**

PROTECT

ENCRYPTION	BACKUP & RECOVERY	ACCESS MANAGEMENT
Encrypt data both at rest and in transit to prevent unauthorized access or disclosure of personal data.	Prepare for events, incidents and disasters by maintaining regular backups and routinely stress test your breach response processes, procedures and technology. Create and test recovery	Define a specific purpose for data before it is collected, use that data only for its intended purpose, and limit access to that data on a "need-to-know" basis to fulfill that purpose.

	plans to bring data and operations back online efficiently and effectively.	
□ **Is any of the personal data controlled or processed by your organization vulnerable to breach?**	□ **How long would it take your organization to identify, contain and address a data breach incident?**	□ **Has your organization increased its risk by allowing more people to access data than truly need it?**

GOVERN

RECORD OF PROCESSING ACTIVITIES	DATA MINIMIZATION	DISCLOSURE/TRANSFER
Keep detailed and current records of the systems on which your data is stored, the types of data stored on those systems, the sensitivity of that data, who is responsible for those systems, the retention cycle for the data, and activities your organization is conducting with the data it collects.	Don't engage with more data than you need to. Limit your collection of data to only what is needed for a specific purpose, don't collect data "just in case" you might someday need it, and don't use the data for purposes other than that for which you collected it.	Carefully address the processes, procedures and risks for data leaving your organization. Govern your data sharing practices in line with contracts and consent. Don't transfer data to an organization that won't protect it.
□ **Do your organization's processing activities align to the consent provided by an individual for that data?**	□ **Do you truly need a consumer's Social Security number to provide a service?**	□ **Are your service providers applying the same level of data protection and governance as your organization?**

ENABLE

NOTICE & CONSENT	PROCESS RESTRICTION	ACCESS & ERASURE
Enable individuals to maintain and exercise control over their data through notice and consent practices. Enact straight-forward policies, written in plain language, to alert individuals as to what data your organization collects and why you are collecting it. Obtain the necessary consent for the purposes you disclose.	Respect an individual's right to limit the way your organization uses their data, as well as with whom you share their data.	Develop procedures for individuals to request access to the data you hold about them, to obtain a copy of that data, and, if they so choose, to request that you delete their data.
□ **Do you use data from consumers/customers for a purpose for which they are not aware nor have consented?**	□ **Does your organization have a procedure in place to respond to an individual's request to restrict processing as required by applicable data privacy regulations?**	□ **If an individual requested that you delete their data, would you know all the locations where their data may be stored?**

*****

Kral Ussery LLC serves US public and private companies to protect and grow shareholder value, as well as non-profits and governments with internal controls and in combating fraud. We assist entities in all matters relating to financial reporting, including SEC compliance, internal controls, SOX-404, IT general controls, IPO & SPAC readiness, M&A transactions, US GAAP compliance, audit preparedness, technical accounting memos, and valuations/PPAs. Visit us at www.KralUssery.com.

This is an article from the Governance Issues™ Newsletter, Volume 2022, Number 3, published on October 25, 2022, by Kral Ussery LLC.