WRANGU

12 Elements for an Effective Data Protection Management Framework

WRANGU

This Framework can be used as a guide to achieve and demonstrate compliance with Fair Information Practice Principles, data protection and privacy laws.

Data Protection Governance

- Create a data protection organization vision
- Define the scope of a data protection program
- Choose a relevant data protection framework
- Choose a data protection risk and compliance management tool
- Develop a data protection strategy
- Set up a data protection team
- Choose a data protection governance model, i.e., centralized, decentralized, hybrid
- Create a reporting structure
- Identify and engage stakeholders throughout the organization
- Conduct regular roundtables

Requirements and Practices

- Identify ongoing data protection compliance requirements: i.e., laws, regulations, codes of conduct, etc.
- Identify applicable laws, regulations, compliance requirements: GDPR, CCPA, POPIA, LGPD, PIPL, etc.
- Identify commonalities and differences in the applicable laws, regulations, compliance requirements, etc.
- Identify third-parties external data protection resource: i.e., privacy legislation software, privacy professional associations, newsletters, conferences, roundtables

WRANGU

Inventories of Data

- Create and maintain records of the processing activities to obtain and prioritize resources, efforts, risk assessments policies in response to incidents and demonstrate accountability and compliance
- Organize the records of the processing activities around the data life cycle: collection, usage, transfers, retention, and destruction
- Document data flows: i.e., by using a data flow mapper
- Classify data type: i.e., public, client, partner, supplier, internal, sensitive, highly sensitive
- Identify technological and organizational measures
- Identify types of data subjects
- Identify cross-borders and international data transfers
- Identify the lawful basis for processing

Data Use Policies and Notices

- Define a policy which governs the goals and strategic direction of the organization's data protection office
- Set out controls to achieve policy goals
- Include details on the operating processes and procedures used on the ground to achieve policy statements
- Set out retention policies and schedules
- Put in place a data destruction procedure
- Have a disaster recovery and backup policy
- Maintain a data protection by design and default policy
- Put in place a BYOD policy to govern the use of i.e., mobile devices, home, and remote working
- Communicate the policies within the organization
- Maintain data privacy and cookies notices

WRANGU

Training and Awareness

- Develop training materials to reinforce the organization's data protection policies and practices: i.e., classroom training, online learning through streaming, videos and websites, poster campaigns, booklets, workshops
- Training is a key control, and under some regulations (i.e., HIPAA) is a requirement
- Training should address applicable laws and policies, identify potential violations, address data protection complaints and misconduct, and include proper reporting procedures and consequences for violating laws and policies
- Where appropriate extend internal training to business partners and vendors
- Require trainees to acknowledge in writing that they have received training and agree to abide by company policies and applicable law
- Repeat trainings and create new training opportunities at regular intervals

Data Assessments

- Conduct maturity assessment to measure the company compliance with laws, regulations, adopted standards and internal policies and procedures
- Conduct Privacy Impact Assessments (PIAs) associated with processing personal data in relation to a project, product, or service
- Conduct Data Protection Impact Assessments (DPIAs) to identify risks arising out of the processing of personal data and to minimize these risks as much and as early as possible
- Conduct Transfer Impact Assessments (TIAs) to gauge the efficiency of the transfer mechanisms tools in the country of destination
- Conduct vendor's assessments through questionnaires, privacy impact assessments and other checklists
- Conduct mergers, acquisitions, and divestitures privacy checkpoints
- Conduct lawful basis assessments: i.e., consent validity assessments, Legitimate Interest Assessments (LIA)

WRANGU

Data Subject Requests and Complaints

- Facilitate for the data subject's requests in connection to their rights: right to transparent communication and information, right of access, right to rectification, right to erasure, right to withdraw consent, right to restrict processing, right to data portability, right to object, right to not be subject to automated decision-making including profiling
- Work with the legal team to establish policies and procedures that align with legal requirements
- Have a documented process and follow it to define and enable mechanisms for: differentiating between sources and types of complaints, designating recipients, have a centralized intake form, track the process, report and document decisions and redress measures
- Train your personnel to identify data subject's requests and complaints since they can come though different channels, such as email, phone, social media

Data Security

- Ensure the confidentiality, integrity, availability, and resilience of data throughout the data life cycle
- Identify risks, select, and implement controls and measures to mitigate risks, track and evaluate risks
- Implement information security standards and guidelines for consistent application of management, technical, and operational controls to reduce the risks to confidentiality, availability, and integrity of data
- Work with IT to ensure effective access controls, at least the basic security principles for role-based access controls (RBAC): segregation of duties, least privileged, need-to-know access
- Classify data based on the risk to the business in the event of unauthorized access or loss of the data
- Implement technical controls such as obfuscation, data minimization, security, Privacy Engineering Technologies (PET)

WRANGU

Data Breach Response

- Create a data breach response plan which can be part of the company's larger incident response plan (including roles by function)
- Register the breach with the remedial action taken
- Notify, if required, the relevant authorities and the affected individuals
- Create and maintain a vendor management plan to mitigate potential breaches caused by vendors
- Integrate the response plan into the business continuity plan
- Allocate budget for training and response

Third Party Risk

- Have specific standards and processes for vendor selection
- Create standard intake forms to check on a series of criteria such as, vendor reputation, financial condition, insurance, information security controls, points of transfers, disposal of data, incident response, employees training, audit rights, sub-processors
- Create contractual language to satisfy the regulatory requirements and internal policies
- Put in place processes for reporting and record keeping, ongoing monitoring, and vendor offboarding

WRANGU

End of Life Cycle

- Terminate employee's and consultant's contracts
- Inform IT and facilities to cease immediately or simultaneously the physical and electronic access
- Wipe out phones, equipment, and other employee devices together with login and password credentials
- Create a procedure for retrieving portable storage devices or media from departing employees
- Revoke access, delete accounts, keep records, and perform audit against accounts

Auditing Program Performance

- Track and benchmark through performance measurement products, services, and systems
- Conduct internal and external audits including reviews of people, processes, technology, finances, and other aspects of business functions
- Track details about the type and origin of complaints and their handling
- Track the type of breach, severity, and time to remediation to determine if training activities and program processes are sufficient
- Pick-up gaps and provide foundation for remediation planning

WRANGU

Petruta Pirvan
Head of Privacy and Compliance

Stephen Ragan
Principal Privacy Consultant

Contact Us

Wrangu provides trusted advisors to accompany businesses on their path to comply with different laws and regulations.

Please feel free to get in touch with our experts.

Website:
www.wrangu.com

Email:
hello@wrangu.com