Association of Corporate Counsel
U.S. States' Privacy Laws Capability Maturity Model

Maturity Model Overview

The Association of Corporate Counsel U.S. States' Privacy Capability Maturity Model provides a detailed maturity model for all aspects of an organization's privacy program. It seeks to gauge program capability across a variety of program elements, taking a "big picture" view on how ready organizations are to comply with these requirements.

Privacy Capability Program Objectives

Effective privacy programs are a combination of policies, processes, technology implementation, training, monitoring and auditing to identify, classify, secure, manage, and delete sensitive information across electronic and paper media. This Capability Maturity Model seeks to calibrate an organization's capability and readiness to meet the demands of current and new privacy requirements.

This model defines "capable" in the following ways:

Ensure Compliance – Ability of the organization to meet a wide variety of legal and regulatory privacy requirements
Reduce Risks – An organization's ability to reduce potential privacy-related risks, such as mitigating the potential for data breaches, negative publicity, A7 regulatory actions and fines
Operability and Scalability -- Ability to compliantly manage privacy information in an efficient and effective manner, as well as scale privacy processes
Flexibility – Ability to meet new or changing privacy requirements
Cost Effectiveness – Ability to do all the above in a cost-effective manner

Background information on the concepts outlined in this Model is available in the ACC InfoPAK: "Complying with New and Emerging U.S. State Privacy Requirements." This InfoPAK as well as other privacy and Information Governance information is available on the ACC Information Governance Network Website page or upon request at info@contoural.com.

Model Notes

U.S. State Privacy requirements are rapidly emerging and evolving. It is possible that recently enacted regulations may include requirements not explicitly addressed by this model. For example, some privacy regulations require the appointment of a Chief Privacy Officer while others do not. However, this model takes a broad approach that should be applicable to all or nearly all aspects of these requirements. Not all aspects of this model will apply to every organization.

The reader should keep in mind that the amount and diversity of privacy information varies from organization to organization. As such, the importance of any given capability is likely to vary from organization to organization, based on the weighting of various maturity aspects. Also note that this model focuses on the overall capability and readiness; it does not address the best strategy for achieving a capability. While this model touches on other aspects of Information Governance programs, such as records management or litigation readiness, it does not specifically address those areas. Finally, the model is ordered based on program workstreams, and not by the relative importance of any given capability.

Disclaimer: Contoural provides information regarding business, compliance and litigation trends and issues for educational and planning purposes. However, legal information is not the same as legal advice -- the application of law to an individual or organization's specific circumstances. Contoural and its consultants do not provide legal advice. Readers should consult with competent legal counsel for professional assurance that our information, and any interpretation of it, is appropriate to each reader's situation.

Privacy Policies and Notices

Maturity Model Criteria	Level 1 – Immature	Level 2 – Limited	Level 3 – Essential	Level 4 – Proactive	Level 5 – Advanced
Privacy Policies	Privacy policy is either informal or non-existent	Privacy policy is either not fully documented or incomplete; policy may exist for a single regulation, but not for newer regulations; no attempt has been made to customize the policy to meet the organization's current requirements	Privacy policy exists and documented; policy addresses and covers all applicable regulations; policy has been customized to fit the organization's current and specific requirements	+ Policy is regularly reviewed and updated; policy includes any specific regional requirements or emerging regulations	+ Fully developed and normalized policy across all geographies, jurisdictions, and emerging regulatory frameworks
Privacy Notices	Notice not provided on a timely, comprehensive or legally sufficient basis; information provided on choice and consent inconsistent with requirements	Notice not easily understood; types of information collected not fully disclosed; consent not always documented per requirements; all forms of sharing not fully disclosed	Notice is provided timely in plain and simple language; types of information collected and shared fully disclosed; choice and consent policies fully documented; privacy notices available to customers or employees at will	Notice regularly reviewed and updated; individual choice and consent preferences are documented, tracked, and audited	+ Continuous improvement to all notices based on changes in law, business practices, and third-party relationships

Privacy Organization and Awareness

Program Ownership	There are no resources dedicated to privacy activities, or are provided on a limited ad hoc basis	Privacy is owned and managed by individual departments or business units	Resources are authorized to provide privacy support throughout the organization	Privacy Organization exists, with dedicated privacy owner; senior-level management aware of and support program objectives	Senior management reviews privacy organization quarterly to evaluate adequacy, availability and performance; privacy capabilities included in risk and board-level reporting
Steering Committee	No coordination on privacy across departments	Limited ad-hoc coordination on privacy issues	Key stakeholders engage on privacy through a steering committee working group chaired by Chief Privacy Officer or other senior executive; steering committee includes participation from business units	+ Privacy executive committee composed of senior stakeholders oversees working group and privacy function	+ Privacy executive committee engages with board audit committee
Privacy Coordinators	Business units have little exposure to privacy	A few individuals liaise with some business units to address privacy questions and issues	Most departments have dedicated part-time privacy coordinators.	All groups across the enterprise have full-time privacy coordinators with dedicated training	+ Privacy coordinators meet regularly and ensure consistency across the enterprise
Privacy Training and Awareness	Formal privacy training is not provided; awareness may come from other employees or outside sources	The organization maintains a privacy awareness ad hoc, but messaging and training are inconsistent	Employees who handle privacy information are trained on privacy principles and responsibilities; completion of privacy training tracked and monitored	All organization employees receive privacy awareness training on a regular basis; additional privacy awareness activities conducted periodically; privacy awareness is tested as part of training	Privacy awareness leads to a strong privacy culture; remedial training is provided when breaches or incidents occur

Information Security and Breach Response

Data Security Policies	No or limited information security program; access controls inconsistent/ incomplete	Limited information security program; no documented data security classification policy	Comprehensive, enterprise-wide information security program including documented data security classification policy based on best practices, but not unique privacy requirements	+ Annual review of information security risk and practices; ongoing audit of policy application to all types of privacy information across all media	+ Annual review of security program for effectiveness; formal risk management program relating to privacy
Incident Monitoring	No incident monitoring in place	Ad hoc incident monitoring	Formalized and documented incident monitoring program and response	+ Continuous monitoring of all access controls and incident logs for continual improvement	+ Monitoring includes utilizations of advanced security technology
Breach Response Plan	No breach response or business continuity plans; no security for data transmission	Limited breach response/ business continuity plans; limited security for data in transmission	Documented procedures for breach response, access controls, business continuity; designated executive assigned who will make decisions in the event of a significant data breach	+ Regular walkthroughs of breach management plan; preapproved data breach response vendors (forensics, credit monitoring, etc.) contracted	+ Formalized and systematic analysis of breach, access attempts and response activities; media plan with draft press releases and a dark page on their website that is ready to go live with information in the event of a significant breach; breach response tabletop exercises completed annually

Structured Data Capability

Structured Privacy Information Identification	Privacy information is not identified in databases or other internal structured systems	Basic data classification of privacy information identified across major systems; no workflows mapped	Privacy information specifically identified, classified and inventoried in all structured enterprise systems; workflow of privacy information across structured systems identified; systems comply with security policies	+ Privacy information also identified and inventoried in any departmental databases or systems	+ Formal system change management process identifies privacy information as new systems are deployed or retired

Structured Privacy Information Security	No procedures for access or security controls of privacy information in internal structured systems	Processes exist for access, and authentication of privacy information in structured systems, but not documented; decisions made by system owners	Structured systems that contain privacy information have access and security controls documented, implemented and monitored	+ Structured systems subject to regular security monitoring and testing	+ Structured systems privacy information monitoring and security testing for newly deployed systems and change management for existing systems
Structured Privacy Information Production	No procedures for production of structured data for access requests under data privacy requirements	Ad hoc procedures for production of structured data for access requests under data privacy requirements	Documented procedures for production of structured data for access requests for enterprise systems	Documented procedures for production of structured data for access requests for departmental systems	+ Easily executable and scalable production processes for producing all privacy information in all relevant structured systems
Structured Privacy Information Deletion	No procedures for deletion of internal structured data for access requests under data privacy requirements	Ad hoc procedures for deletion of structured data for access requests under data privacy requirements	Documented, approved procedures for deletion of structured data for access requests; processes maintain referential integrity	+ Older, expired, unneeded privacy information routinely deleted from structured systems; records of deletion retained	+ Easily executable and scalable deletion processes for structured systems

Unstructured and Semi-structured Data Capability

Unstructured and Semi-structured Privacy Information Identification	Privacy information is not systematically identified in file systems, desktops, email systems, offline or desktop email storage or other unstructured or semi-structured repositories.	Basic categories of privacy information identified in specific locations within larger unstructured repositories and email	Privacy information identified and inventoried for all unstructured and semi-structured data, including systems, repositories and desktops	+ Privacy information identified non-traditional in unstructured or semi-structured media such as wikis	+ Change management process identifies and disposes privacy information as new systems are deployed or retired
Unstructured and Semi-structured Privacy Information Security	No procedures for access of unstructured or semi-structured privacy information; limited or no application of data security processes	Ad hoc processes exist for access, and authentication of privacy information in unstructured systems, but not documented	Ununstructured and semi-structured systems and repositories that contain privacy information have access and security controls implemented and monitored	+ Unstructured and semi-structured systems subject to regular security testing	+ Unstructured and semi-structured systems security testing incorporated into change management for newly deployed systems

Unstructured and Semi-structured Privacy Information Production	No procedures for production of data for access requests under data privacy requirements	Ad hoc procedures for production of unstructured or semi-structured data for access requests under data privacy requirements	Documented procedures for production of unstructured or semi-structured data for access requests for enterprise and departmental systems	+ Documented procedures for production of unstructured or semi-structured data for access requests for departmental systems including individual information stores	+ Easily executable and scalable production processes for unstructured or semi-structured systems
Unstructured and Semi-structured Prviacy Information Deletion	No procedures for deletion of unstructured or semi-structured data for access requests under data privacy requirements	Ad hoc procedures for deletion of unstructured or semi-structured data for access requests under data privacy requirements	Documented and approved procedures for deletion of unstructured or semi-structured data for access requests for all systems	+ Older, expired, unneeded privacy information routinely deleted from structured systems	+ Easily executable and scalable deletion processes for unstructured or semi-structured systems

Paper Information Capability

Paper-based Privacy Information Identification	Privacy information is not systematically identified in either onsite or offsite paper records or documents	Privacy information identified in paper information in speciific locations on a limited, ad hoc basis	Paper-based privacy information identified and inventoried-for all onsite and offsite locations	+ Paper-based privacy information routinely converted to electronic format, and paper copy is destroyed	+ Paper-based privacy information classfied upon initial creation or receipt
Paper-based Privacy Information Security	Little or no physical security applied to documents containing privacy information	Physical security applied to some onsite or offsite paper document storage, but not consistently	Physical security applied to all paper documents containing privacy information	+ Physical security subject to regular security testing	+ Full physical security and access controls applied to full lifecycle of paper documents containing privacy information
Paper-based Privacy Information Production	No procedures for production of paper-based privacy information under data privacy requirements	Ad hoc procedures for production of paper-based privacy information under data privacy requirements	Consistent, documented processes for production of paper-based information	+ Easy and efficient processes for production of paper-based privacy information	+ Fully scalable production of paper-based privacy information
Paper-based Privacy Information Deletion	No procedures for selection and secure destruction of paper-based privacy information under data privacy requirements	Ad hoc procedures for secure destruction of paper-based information under data privacy requirements	Documented, consistent, secure and approved processes for selective secure destruction of paper-based privacy information	+ Easy and efficient processes for secure destruction of paper-based privacy information	+ Fully scalable selective secure destruction of paper-based privacy information

Third-party Data Management Capability

Third-party Privacy Information Identification	Privacy information stored, shared or sold to third parties not identified	Limited identification of privacy information stored, shared or sold to key third parties	All privacy information stored, shared or sold to all third parties identified	+ Third-party privacy information tracked throughout lifecycle, from creation through tranmission, data enrichment, retention, and disposition	+ Formal system change management process identifies all data flows for privacy information to all third-party systems as new systems are deployed or retired through entire lifecycle
Third-party Privacy Custodian Information Governance and Controls	SLAs contain no provisions regarding production, deletion or retention of privacy information	SLAs provide for the discovery and production of information to meet privacy information requests	SLAs provide the capability to discover, produce and delete privacy information upon request	+ SLA sets a specific retention period for privacy information	+ SLA allows for a specific retention period for privacy information to be set to match the retention period of the company at an individual content level
Third-party Partner Privacy Information Service Level Agreements (SLAs)	SLAs contain no provisions regarding proper handling of privacy information; no communications on requirements	SLAs prohibit the selling, retaining, using, or disclosing of privacy information; privacy requirements communicated	SLAs require third party to delete a consumer's privacy information upon request, as well as fulfilling other consumer access requests; agreement covers re-use, enrichment, retention and disposition	+ SLAs require the use of specific security measures (e.g., encryption, anonymization) to protect privacy information; SLAs contain the right to retrieve or request deletion of the data at the end of the contract	+ SLAs require third party to cooperate in privacy audits, privacy impact assessments, and regulatory or legal inquiry

Consumer Access Request Procedures, Monitoring and Enforcement

Access Request Authentication	No method of authenticating identity of consumer	Some process in place of verifying identity, using ad hoc means	Identity authenticated via use of ID and Password used for account, but none if no account	Identity verified through use of industry-recognized authentication standards	Authentication mechanism regularly monitored and audited for effectiveness
Access Request Tracking	Consumer access requests are not tracked	Tracking of consumer access requests is manual and inconsistent	Access request tracking is centralized; at least two separate mechanisms for consumers to submit access request	Access requests are automatically logged, including workflow to respond to the request; full records retained of requests	Continuous improvement of access request tracking processes and technology use

Audit	No procedures in place to audit consumer access request process	Basic guidelines in place to audit consumer access request process, but not routinely followed	Audit procedures are well-defined and published; audits are ad hoc in nature	Consumer access request process is routinely audited	Audit process strives for continuous improvement of consumer access request process

Privacy Program Integration with Other Compliance Programs and Processes

Integration with Records Management	Privacy processes are not integrated with records management Policies, Schedule, or processes or data classification standards	Privacy only addressed in Records Policy but not the Schedule or data classification standards	+Privacy information inventory cross-referenced with the Schedule; privacy deletion requests are synchronized with retention requirements	+Records management and privacy classification occur as a single process	+Automated controls prevent the premature deletion of privacy information that would conflict with legal retention requirements
Integration with Discovery Processes	Privacy processes are not integrated with legal discovery processes	+ Privacy disposition request suspended if in conflict with legal hold	+ Routine privacy destruction processes fully suspended for groups of documents under legal hold	+Automated records destruction processes fully suspended for individual privacy information under legal hold	+Release of legal holds automatically invokes resumption of pending privacy deletion requests

Privacy Program Procedures, Monitoring, Audit, Enforcement and Maintenance

Privacy Procedures	No privacy procedures in place	Privacy procedures established in certain areas, but not well-understood or consistent across the organization	Privacy procedures are well-defined and published	Well-defined and published privacy procedures are reviewed and updated and published on a regular basis	+ Privacy procedures are routinely audited for compliance and fully integrated into the organization
Program Monitoring	Privacy-related issues or concerns are addressed informally; no process to address inquiries, disputes, complaints; no formal compliance program	Processes are in place to monitor for changes, address disputes, inquiries and complaints, and measure compliance, but are not fully documented	Documented policies are in place to address changes, disputes, inquiries, complaints, and monitor compliance	Established process for monitoring privacy environment; disputes, inquiries, complaints addressed in timely manner; management monitors noncompliance	Continuous monitoring and analysis used to improve privacy process; non-compliance results in training and disciplinary action

Program Audit	No privacy-related audits	Limited or ad hoc privacy audits	Scheduled and thorough audits of privacy program policies, processes and requests.	+ Ongoing detailed, "spot" audits of compliance processes, including request and deletion processes; regular data scans searching for misclassified or misplaced privacy information	+ Audit processes built and automated into all privacy processes; audit results communicated through steering committee/key stakeholders
Program Remediation	Ad hoc remediation on specific issues/individuals	Policy acknowledgement tracked and can be escalated	Risks identified and communicated on a regular basis	Risks identified and formal remediation plans developed on annual basis	Internal Audit findings formally tracked and communicated to key stakeholders for sign off
Program Maintenance and Refresh	Limited updates	Policies and processes are updated on an ad hoc basis	Policies and processes updated minimally every 12 to 18 months; trainings are also updated concurrent with the program update	+Privacy requirements are regularly monitored and programs and processes are updated as new requirements are enacted	+On a semi-annual basis requirements that occur are proactively identified and implemented
Change Control Process	No change control process applied to policies or processes	Changes to privacy processes are handled in an ad hoc manner	Audit results are feedback into a change control process that may flag required changes to the policy or processes	+Regular audits are fed into formal change control process	+Formal change management applied to schedule driven by audits from multiple compliance regimes