Privacy Management for Content Systems

prosperoware

Privacy Management for Content Systems: Understanding the Impact of Privacy & Cybersecurity

For any organization that has data in the European Union (EU) or United Kingdom (UK), they are impacted by both General Data Protection Regulation (GDPR) and NIS Directive.

California has a new privacy legislation, the California Consumer Privacy Act (CCPA), which comes into effect in January 2020. New York State just passed a new cybersecurity breach law, and Pennsylvania and Illinois courts created causes of action to sue for breach.

Some of the largest buyers of legal services are also regulated globally for data security and privacy, including financial services, insurance, energy and health care. All these regulations, along with other privacy and cybersecurity laws, include requirements that the regulated entities must ensure their vendors apply similar policies.

The legal and regulatory landscape is only expected to become much more complicated over the next several years. Privacy and cybersecurity laws are very similar. The primary difference is that a privacy law gives an individual more personal rights over their data.

The key point for all of these regulations is that personal data and personal health information should be kept secure and only be available to those who need to use it. In order to reduce risk, destruction of unnecessary private information is needed or data minimization.

Many of these laws are written on the fundamental concept that organizations may experience a data breach. The reality is that nation states are responsible for many of these data breaches. This means that laws and regulations are about ensuring that organizations create appropriate policies or controls, and then making assurances these policies are followed. After a data breach, penalties are levied against organizations that fail to follow these controls.

Organizations should develop clear policies for service deliveries where personal data exists and apply the rules to manage personal data generated during its operations. GDPR and the California Consumer Privacy Act (CCPA) place a lot of requirements:

Privacy by Design

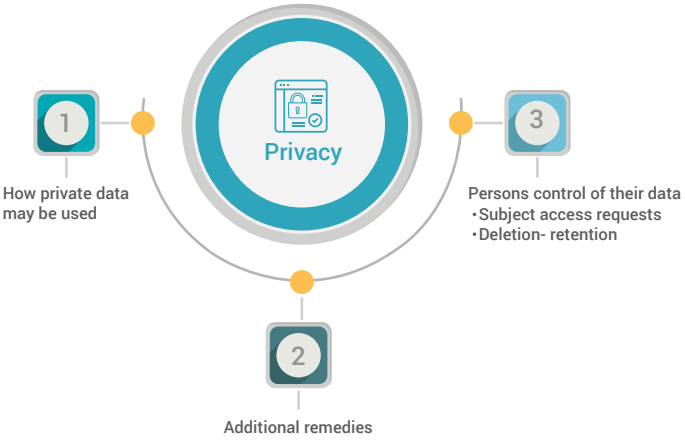
Privacy by design processes and systems manage personal data. This could be a process to secure a particular folder in a workspace for personal data. Businesses should have processes that audit content, ensuring it is being stored in the right place.

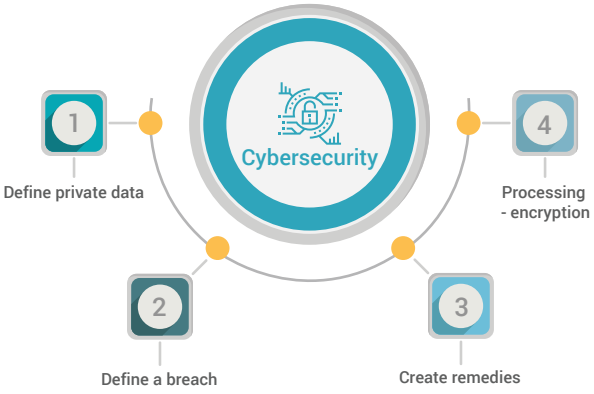
Need-to-Know (de-provision/temporary access)

A core principle of need-to-know privacy laws is that personal data should only be secured to those who need to know and only as long as they need access to perform their duties. While each organization can view this differently, there is a common theme; there are going to be users who need temporary access to content.

When a user changes department, there should be de-provisioning access from no longer relevant department matters and resources. When users leave an organization, their access needs to be cut off and removed.

Similarly, this same philosophy should be applied to administration where service desk, records and administrators are given the least amount of access to perform their duties. Simple examples are the first level service desk not being granted access to document names.





Data Map

A data map is what type of personal data is stored in each system and how it is being used. With content systems, personal data can be everywhere. Building clear process for document and email categorization is essential.

As organizations continue to use more and more systems to manage their content, they need to understand where their data is stored.

Subject Access Requests

In privacy laws, this is the ability for someone to ask what data is being stored. This means that you need the ability to locate all the information for that person and produce it, if required.

GDPR also adds the wrinkle of necessitating the least invasive approach so as not to violate the privacy of other individuals. For firms, this means that they should be ready to track players and parties for each matter.

A matter can be something that has a clear beginning and end (a dispute or a merger) or something that reoccurs annually (regulatory filing).

The process of determining whether documents need to be produced is very similar to transferring a file to another firm or the client.

Data Minimization

The simple concept is to delete or transfer personal data once it is no longer needed in the organization.

Assurance

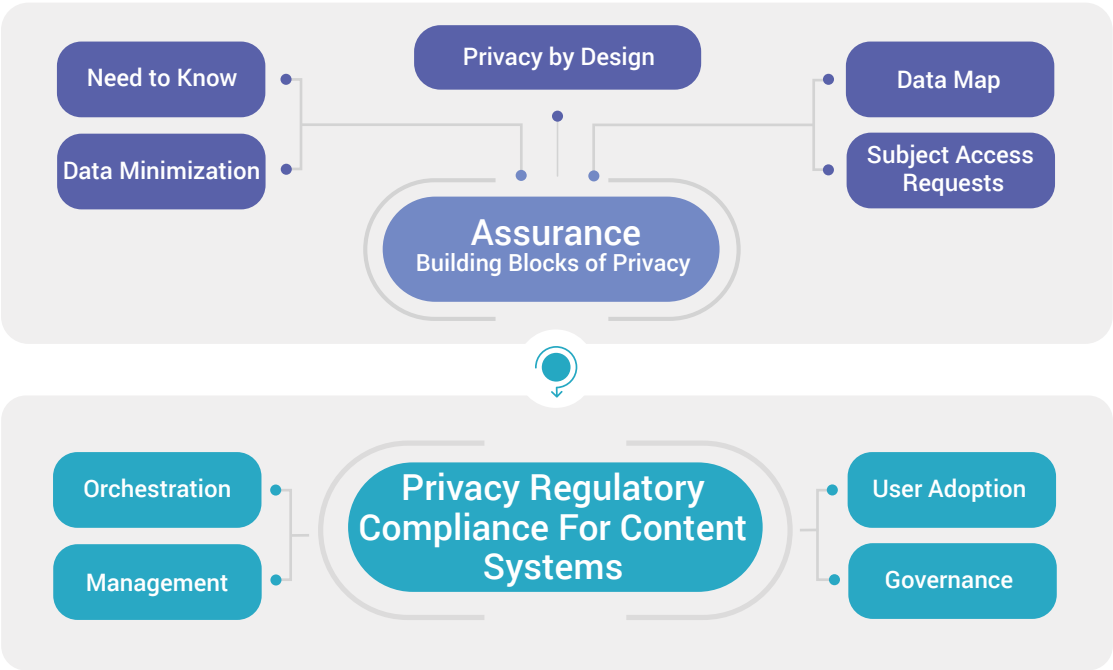
If something happens, the organization will need proof that it has followed its policies.

CAM Addresses the Privacy Challenge Around Content

Aligning people and processes can be problematic without the right technology platform. CAM is a platform for Privacy & Regulatory Compliance for content systems.

CAM's four pillars of functionality are: *(1) User Adoption, (2) Orchestration, (3) Management,* and *(4) Governance*. CAM supports multiple systems, including iManage, NetDocuments, Kira, HighQ, Microsoft Teams, and SharePoint. It also supports orchestration between cloud-based systems such as Salesforce, Clio, and eBilling, among others.

CAM provides organizations with a comprehensive information governance plan to comply with current and upcoming privacy laws and regulations. It allows organizations to *(a) locate their data, (b) understand their data, and (c) ensure data access,* security and management in compliance with privacy regulations and organization's business needs.



Enabling Privacy by Design

The proper organization of documents into matters is the first step in Privacy by Design. Many content systems provide a way to group data into a matter. They may call them sites, workspaces, channels, or some other name. But they will then a contain a set of folders where the documents can be organized.

The folder structure should be designed to enable the grouping of documents to fit the process. The folders are intended to contain personal data, which can then be secured appropriately.

There are two fundamental challenges of creating new matters and making sure users put the data in the right place. **CAM addresses both of these challenges by:**

- *Orchestrating the creation of the matter workspace from time & billing, practice management, CRM, or similar system, or the creation of a matter workplace through a form*
- *Automatically updating the matter workspaces when changes are made in the source system*
- *Enabling a standard set of folders structure that are based on the type of matter*
- *Creating matter teams from time entries and managing the members in that group*
- *Ability to secure folder or entire matter workspaces to a matter team or group*
- *Enabling users to add pre-defined optional folders with an added prefix and suffix, or custom name to aid in the standardizing process*
- *Reporting on usage*
- *The ability to adjust the matter workspace structure to improve usage.*

Management: Need to Know & Other Actions for Service Desk and Administrators

Most organizations use multiple content systems. There are numerous processes where administrators or service desks need to make changes in bulk or on a single document. These range from moving documents between matters, moving matters between physical locations (e.g. USA to Europe), moving content between content systems, change security and document profiles, importing and exporting content. These operations are critical for business operations.

The challenge is to enable a need-to-know approach to service desk and administrative operations. Except for export and import operations, an administrator does not actually need access to the actual document.

For content systems that have document identifiers, the administrators and service desk do not need to see the document name. Similarly, commands available to administrators and service desk users can be similarly limited to their roles. All of these operations need to be audited and linked to the appropriate service desk or workflow tickets.

CAM provides a common layer for administration of content systems and addresses these requirements by:

- *Form-based searching for matter workspaces and documents*
- *Granular security model controlling what action administrators can perform*
- *De-provisioning and provisioning security/access across multiple content systems*
- *Updating document profiles*
- *Moving documents between and within repositories*
- *Exporting documents*

Subject Access Requests

Subject access requests identify matters where an individual may be involved. Organizations must locate relevant documents across multiple systems and all those containing personal data. Equally important is providing third party vendors with the ability to identify stored data.

Organizations need the tracking capability to determine what content should be provided to the requestor in a timely manner. Having safeguards on what content is shared and who has the permission to do so is central to complying with subject access requests.

CAM enables tracking requirements through:

- *Supervision of access for the content shared with internal and external vendors*
- *Role-based access to data ensuring proper security workflow*
- *Simple and intuitive user interface, enabling a clear process to handle subject access requests*
- *Ability to locate and produce relevant data in a timely manner ready for export to external parties*

Data Minimization

Data minimization is the ability to build a schedule that moves or deletes data when it is no longer needed. This is done by implementing a set of policies to eliminate personal data when it is no longer needed for a particular business process.

Many times, this is a multi-step process where content is first moved from one system to another. By eliminating data that is no longer needed, firms reduce risk.

In creating a data minimization policy, organizations should go through a rationalization process where they determine how long data needs to be kept. The should balance the risk of keeping the data versus other legal duties or other purposes for keeping the data.

CAM enables organizations to demonstrate that the appropriate practices of data minimization are in place through:

- *The creation of policy that trigger from matter start or end*
- *Allowing content to be moved between and within systems*
- *Permitting different policies linked through the metadata of the matter*

Assurance

The assurance process provides appropriate reporting to demonstrate that an organization is following its policies. This reporting should address both, user access to data and administrative access to data and changes.

CAM enables:

- *Reporting on audit trails of sources systems and also CAM activities, including services desk and application of data minimization policies*
- *Automated reporting through automated email alerts*
- *Configurable dashboard to monitor activities.*

About Prosperoware

We are a thought leading software enterprise company for a digitized legal industry. Our core competency is our expert understanding of the enterprise systems, the data and processes in legal, and building technology for transformative change. We develop software for cybersecurity, privacy, and regulatory compliance for content systems, and financial matter management.