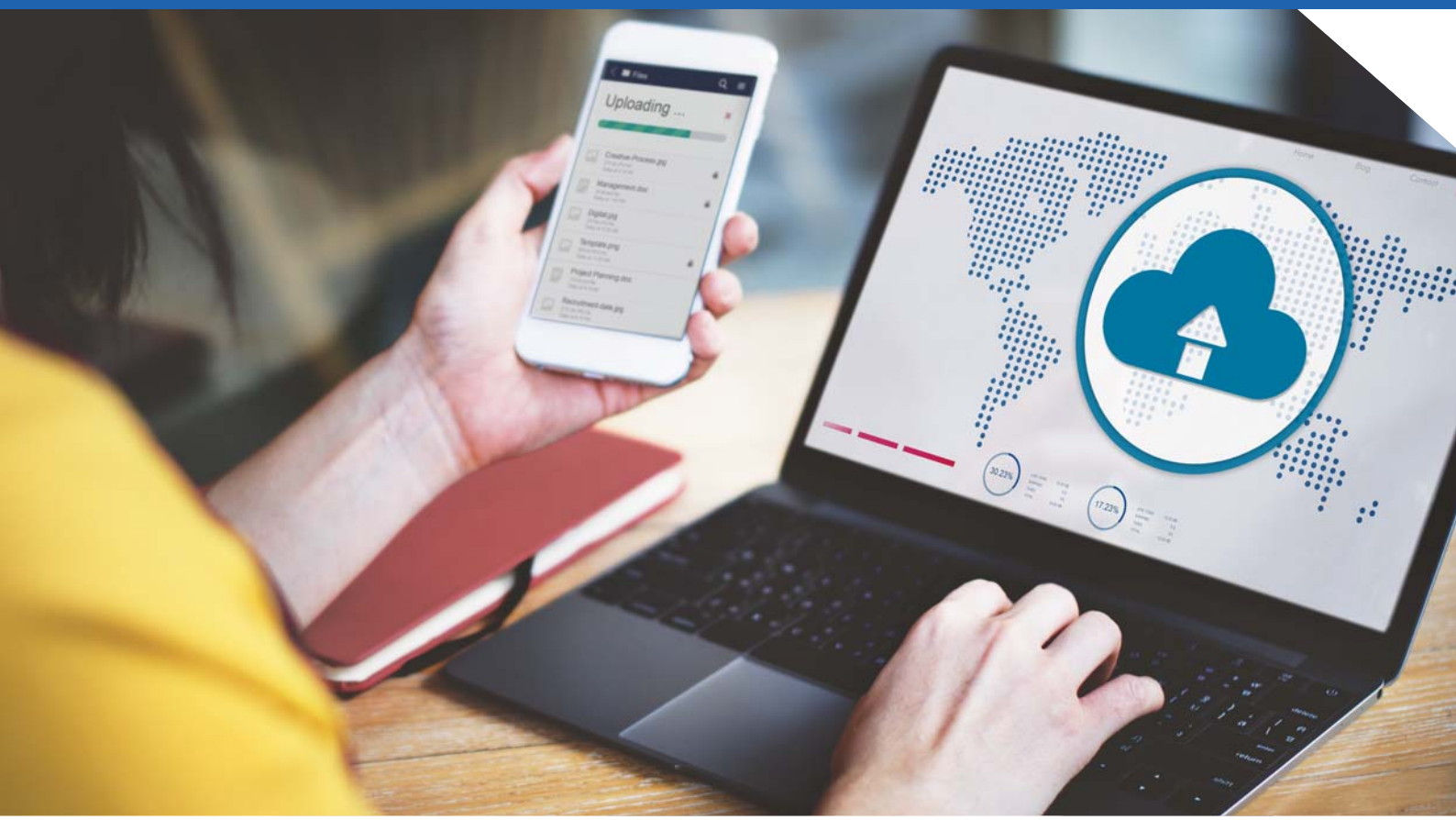
Google Drive

GlassIG
Information Governance

GlassIG

Information Governance for Google Drive



GlassIG is an Information Governance solution used to manage information policies and power organizations' legal and regulatory requirements related to data retention and information lifecycle management.

Unlike alternative solutions, with GlassIG, companies can create corporate policies that are actively managed and published across organizational, jurisdictional and information repository boundaries. GlassIG can be deployed as both a cloud-based or on premise application.

At GlassIG, we simplify Information Governance.

Comply with information policies and apply retention rules for all your content in Google Drive

Google Drive makes it easy to store files in the Cloud and collaborate on shared content. As a result, companies are seeing an explosion in content volume. Not only does this increase storage costs, but it also makes it difficult for companies to comply with business policies, operational costs, and legal requirements. Your organization needs to know what information it has, what it needs to keep, for how long it needs to keep it, how it is used, what value it provides, and what can be disposed of. Unfortunately, Google Vault retention capabilities are not supported in Google Drive[1].

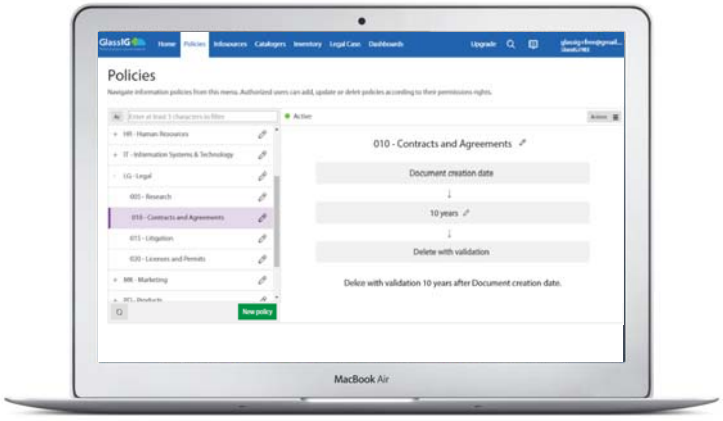
Taking an information inventory allows you identify your information assets and categorize them for future use. In addition, you can identify work in progress (WIP) to act upon at a later time, and redundant, outdated, and / or trivial content (ROT) that provides no value and should therefore be disposed of immediately. Performing such an inventory is a crucial first step in most enterprise-level Information Governance initiatives. Information governance projects then operationalize the policies by which information should be controlled, enforcing those policies on content stored on Google Drive, and measuring the effectiveness of the program.

Preserving Sensitive Content on Google Drive

Companies usually preserve content for a particular period of time in accordance with corporate retention policy. Additionally, content may be preserved at the request of a regulator, legal counsel, or Court as potentially responsive to a pending or active legal or regulatory matter.

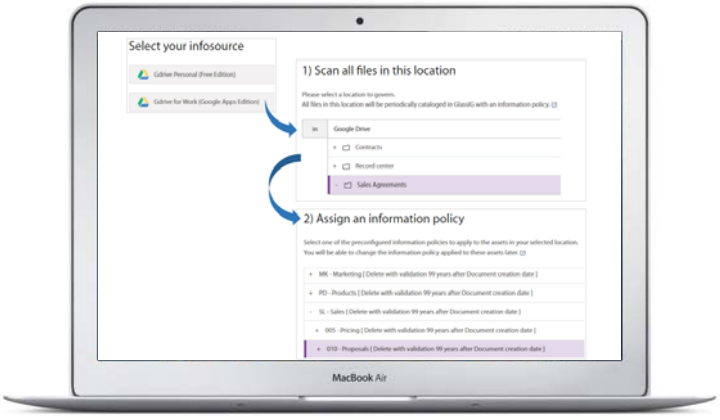
Companies that maintain sensitive content on Google Drive are struggling with how to manage this information in accordance with legal and regulatory requirements. It is not easy to protect or preserve Google Drive content, ensuring that information assets are not accidentally or deliberately modified or deleted. GlassIG helps organizations to comply with information policies, preserving content for legal purposes, while enforcing retention rules on files in Google Drive. GlassIG governance controls may be enforced on Google Drive Personal and Google Drive for Business (Google Apps).

How Does It Work?



With GlassIG, information professionals and compliance managers develop and maintain their corporate information policies outside of Cloud storage system. These information policies are structured into a hierarchy corresponding to the information classes used by the organization and its functional domains, and include the retention rule to be applied on the content. Retention rules define how long your company retains in Google Drive (and, as necessary, other storage platforms). You define retention based on the legal and / or business requirements. GlassIG Defines lifecycle rules as a combination of Event / Time Period / Action. By default, retention is calculated based on Document Creation (an Event). You can also specify other Event types, including business-related events like "End of Contract", "Document Protected" (declared as Record), or "Account Closed". The Time Period then defines when the Action (for example, "Delete with validation") should occur. You may redefine existing retention periods as needed, applying the change to all information assets covered by this policy immediately, retroactively, or at a future date.

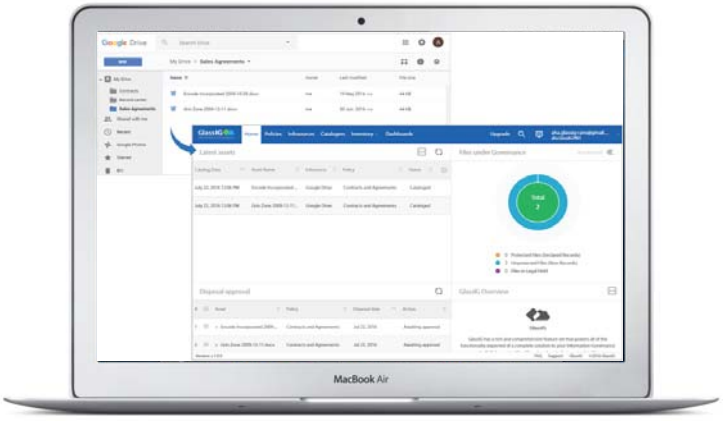
Applying Policies to Google Drive Content



Once Information Policy has been approved, you apply policies to your content by connecting to Google Drive and cataloguing files. The 3-step process takes just minutes:

- Connect GlassIG to Google Drive as an Infosource.
- Point GlassIG to a drive, folder, or subset of the Google Drive hierarchy. This creates a GlassIG Cataloger, which crawls Google Drive directories and sub-directories, extracting metadata required for governance purposes.
- Assign a policy to information assets found within the specific directories.

Content Access, Ownership and In-Place Governance



GlassIG governs your content "in place". That is, GlassIG does not host your files, it simply indexes and references them. Your information assets remain in Google Drive. Google Drive users (individuals and organizations) own their files. Google does not expose any means for third party individuals or technologies to assume ownership, lock down, or preserve a file. This restriction has made it very difficult for organizations to extend their governance and retention policies to Google Drive Content. GlassIG implements the notion of a Preservation Center, allowing GlassIG to move or copy the file and to a designated preservation center. Because GlassIG maintains the policy and governance metadata outside of Google Drive, a preservation center can be located in Google Drive or another governable repository such as Box.com, SharePoint, Amazon, Shared Drives, etc.

Benefits

GlassIG Information Governance for Google Drive enables your company to:

- Comply with retention and legal requirements as defined in your corporate policies
- Deploy end-to-end Information Governance for Shared content on Google drive and other common collaboration systems and cloud-based repositories
- Increase your return on investment in storage platforms by eliminating unnecessary, redundant, obsolete, and trivial content that should be deleted
- Remediate files containing potentially sensitive data
- Ensure defensible disposition for all records stored on Google Drive, Shared Drives, and other storage systems
- Promote accountability across records management, legal, IT, business
- Implement your governance program without migrating content, eliminating impact on IT and end users

[1]See https://support.google.com/vault/answer/6093005?hl=en&ref_topic=3209998