Data is exploding. A recent Veritas report found a 39% average growth per year, with a 9% storage velocity. Storage requirements are outpacing the creating of individual files. By combining statistics like these, however, with an ingrained perception that storage is cheap, you can easily perpetuate the misguided belief that it’s okay to keep everything forever. It’s not, especially in these days of growing regulatory compliance. New and emerging mandates are forcing many to rethink keeping every bit of data forever, even where it can be done in a cost-efficient manner. The sweeping, new General Data Protection Regulation (GDPR), will institute stringent data management requirements, setting precedent and expectations around the world. Though the regulation is not slated to take effect until May 2018, organizations doing business in the European Union (EU) must plan for it today and factor in the many considerations surrounding information retention.

Can I use my backup solution to solely manage information retention enterprise-wide? How do I address non-traditional sources that can communicate personally identifiable information (PII) – for example, instant messaging and social media? How do you determine what information to keep and what may be deleted? And after I figure that out, how do I keep it for only as long as I need to? Finally, do my data management obligations differ if I maintain my information in the cloud versus on-premises? These are some key questions to address as you develop your plan for achieving GDPR compliance. Simply put, to keep information for longer than needed without proper and substantiated context could indeed set you up for significant penalties for non-compliance.

In terms of data minimization, Articles 5, 17 and 32 provide some guidance on retaining personal data in a GDPR compliant store where retention and deletion can be easily managed. Putting processes and technologies in place to help ensure the company is continually applying best practice information governance principles to the use and storage of personal data will be critical and required to prove compliance.

The GDPR discusses three core capabilities related to minimizing your data:

1. **Identification and retention**: Organizations must ensure persona data is kept in a form that permits identification of the data subject for only as long as is necessary. This implies precise understanding of where pertinent data resides and the ability to store that data only as long as needed to meet business or regulatory information retention requirements.

2. **Right to be forgotten and to erasure**: EU residents will have the right to have personal data relating to them erased and further dissemination stopped. This implies an ability to search for pertinent data and mark it for deletion at the behest of a residents or at the end of its useful lifecycle.

3. **Identification, response to and acknowledgement of breaches**: The acceptable timeframe for breach notifications is accelerated and demands that organizations get proactive about predicting and preventing these data crisis. This can be augmented through the ability to monitor electronic communications.

**BACKUPS ARE FOR RECOVERY; ARCHIVING IS FOR DISCOVERY AND MORE**

Similar to rethinking long-term information retention strategy, organizations must also rethink data protection strategy in support of GDPR expectations. While protecting personal data from breach, loss or damage is reinforced in Articles 5, 25, 32, 33, 34 and 35, backup alone cannot efficiently and effectively address the full spectrum of information retention and disposition requirements of the GDPR for a number of reasons. For example, many backup solutions store information based on metadata, such as file owner and date modified. With this in mind, what if you had to address a GDPR inquiry involving searching content based on a Microsoft Word document or PDF document embedded within an
email? How cumbersome would it be to perform such a search if you're only tracking email envelope metadata rather than content embedded within email? In addition, many backup solutions manage retention per backup job versus per individual file.

Assigning retention at the file level during backup in order to meet GDPR record retention requirements would be extremely difficult if not impossible. That's why many companies implement an archiving solution, such as Veritas Enterprise Vault™, which performs content-based indexing during the archiving process. Granular search and retrieval is enabled across all archived information, typically without having to restore items to their original storage location. And this allows organizations to refocus backup on its primary directive – protection and recovery of critical data or systems – while relying on archiving to help simplify long-term information retention, streamline eDiscovery processes and improve regulatory compliance. Not surprisingly, a recent Enterprise Strategy Group survey highlighted “compliance with record retention policies” as the primary factor driving information archiving. See graphic below.

Factors driving organizations to implement archiving solutions
*ESG Brief, Long-term Retention Strategies, to be published.

ONE REPOSITORY FOR LONG-TERM INFORMATION RETENTION

Personal data can reside almost anywhere. Fortunately, Enterprise Vault supports archiving a variety of information sources both natively and through integration with solutions from an extensive, validated partner ecosystem. The benefit is customers are more equipped to track and manage meaningful information no matter where it originates or resides.

Originally developed for archiving Microsoft Exchange Server, Enterprise Vault supports mailbox and journal archiving for both Microsoft Exchange and IBM Domino. Journal archiving is an important consideration when you realize users can permanently delete email on Exchange. To address this behavior, some place all mailboxes on litigation hold forever, but this is not feasible for many and runs contrary to the GDPR position of keeping information “…in a form that permits identification of the data subject for only as long as is necessary.” Journal archiving captures all Exchange sent and received email, independent of user behavior.

- Native archiving support for Microsoft Exchange Server, IBM Domino, Microsoft SharePoint.
- Broad non-native archiving support via Veritas Technology Partner Program solutions, including the following and more:
  - Social media platforms such as Facebook, Twitter and LinkedIn.
  - Instant messaging platform such as Skype, Cisco Jabber and Yahoo Messenger.
  - Collaboration platforms such as Yammer, Salesforce Chatter and Jive.
CLASSIFY TO CULL MEANINGFUL INFORMATION FROM GARBAGE

Classification is critical in helping customers to determine what information to keep and what may be deleted. As a built-in feature for Enterprise Vault, manual classification enables users to drag desired email and files into folders with predefined retention that supersedes established retention policy. For such an action, you trust users to make the appropriate decisions for retaining information for a prescribed amount of time. To remove the guesswork, however, Enterprise Vault also supports automated classification of any content it can archive. Customizable classification policies – see graphic below – enable specific actions during the archiving process: assign a unique retention period or tag with metadata for faster search or supervision.

Over time, retention policy can and often does change. Enterprise Vault supports re-classifying archived content to meet evolving business and regulatory information retention requirements. Re-classification may also be used to help streamline migration to a new archival storage platform or to the cloud. And when archived information is set to expire, Enterprise Vault may be configured to confirm expiry with current policy. Administrators can opt to let expiry and deletion continue as planned or reset retention. This may be accomplished broadly or granularly at the archived item level. Enterprise Vault and its classification capabilities help customers achieve greater precision and confidence in how they manage long-term information retention and disposition in support of GDPR mandates.

CLOUD DOES NOT ABSOLVE YOU FROM RESPONSIBILITY

Where are you in adopting the cloud? Many already are running cloud-based enterprise-wide applications, such as email, file serving and collaboration, while others are actively planning their migration. Regardless of the business reasons driving your organization, understand your obligations for protecting personal data and privacy in the context of GDPR do not change as you transition away from on-premises infrastructure. With this understanding, view cloud migrations as an ideal opportunity to take control of your unstructured data, align with GDPR expectations and leverage Veritas Enterprise Vault as your foundation to renewed information governance.

- Archive first to reduce storage footprint, helping streamline and simplify the migration process.
- Use classification to identify and prioritize what information must be migrated.
- Delete data deemed no longer business-relevant and expire redundant, obsolete or trivial information.
- Leverage flexible deployment options – maintain Enterprise Vault on-premises and archive content to the cloud, or transition Enterprise Vault to a public cloud, helping preserve investment and skills.
GDPR COMPLIANCE STARTS WITH GLOBAL VISIBILITY

Organizations today need to manage their data as a critical asset, with solutions that reliably protect the right data, ensure resiliency and on-demand access from anywhere and reduce the risks and costs of storing their ever-increasing amounts of data throughout the globe.

360 Data Management for GDPR provides the framework for your organization to put data governance at the core of your digital transformation strategy. Veritas takes an integrated approach to solving the GDPR challenge. By combining many of its market leading information intelligence, protection and resiliency products and services, Veritas is uniquely positioned to help you tackle these steps in your journey to GDPR compliance.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies LLC enables organizations to harness the power of their information, with solutions designed to serve the world’s largest and most complex heterogeneous environments. Veritas works with 86 percent of Fortune 500 companies today, improving data availability and revealing insights to drive competitive advantage.