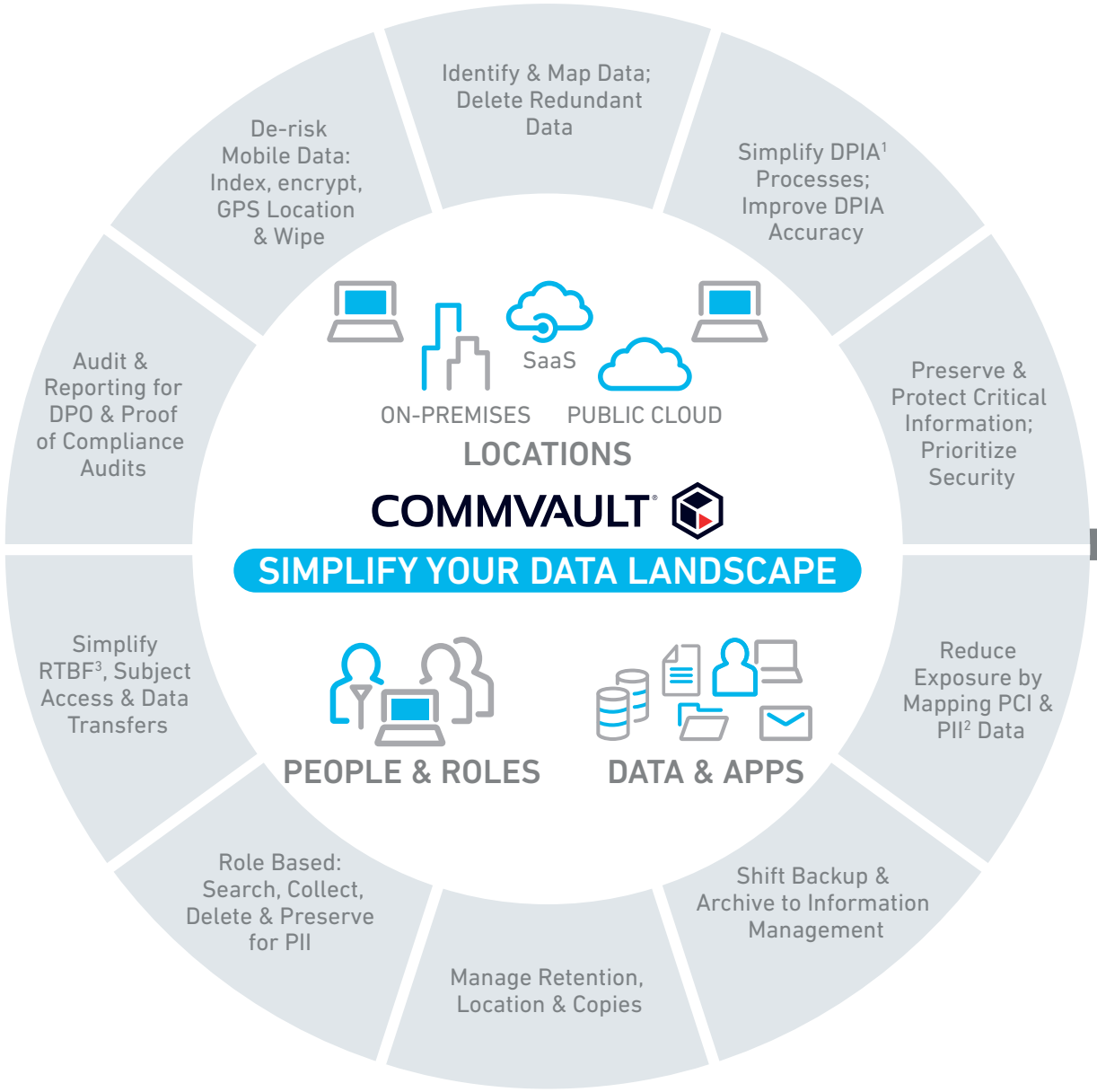
COMMVAULT®

A Simple Guide to GDPR Data Management

GDPR PRINCIPLES	THE DATA CHALLENGE	COMMVAULT VALUE
Right to be forgotten (RTBF, Article 17)	An individual will have the right to ask a business to 'forget them' so that contact is broken. This means personal data must be deleted, but not records that should be legally retained e.g. financial transactions	Commvault software has the ability to content index data in backups, archives, file systems and endpoints, and can search common databases and SaaS offerings in place, making it much easier and less costly to find personal data. Once found, PII data can be reviewed and securely erased as necessary
Data protection by design and by default (Article 25)	The systems and processes that manage data should be designed from the outset with the regulations in mind, so an individual's data is protected at creation/collection and throughout its lifecycle. It means protection in every sense: against misuse, with security measures and with regard to backup and availability	The broad coverage of on-premises and cloud systems supported by Commvault's backup and archive tools, combined with sophisticated automation, mean that all of your systems are protected by default. Encryption can be enabled end-to-end, and a strong security model with auditing and role based management & access are all also 'on by default'
State-of-the-art (SOTA) (SOTA, Articles 25 & 32)	Many of the privacy laws prior to GDPR were written before the likes of FaceBook existed. This principle challenges organisations to continually review whether processes and tools are keeping up with change (and improve if required) to avoid the need to continually review legislation	Commvault has a track record of early support for many new and developing technologies and standards e.g. containers, open source, flash, big data etc. In addition to this, the Commvault platform approach is unique by design; the single index, cloud and SaaS capabilities, app and storage support and more
Security and ensuring confidentiality, integrity, availability and resilience (Article 32)	This part of the regulation is self explanatory. Organisations need to know where their GDPR-related data lives, both on-premises and in the cloud. With that visibility they need to be able to at a minimum encrypt that data, remove it from where it shouldn't be and minimize copies of it. In addition, organizations must be able to ensure accessibility and be able to restore quickly.	Commvault has an advantage over multiple point products, or acquired portfolios, because it provides a single window into high-value enterprise data. From here users can find, encrypt and remove data from the production systems, set retention policies or erase; establish role-based access, and track and report on all actions taken. Commvault also adds a layer of ransomware alerting on laptops and in the datacentre, and can remotely wipe lost laptops
72 hour data breach notification (Articles 33 & 34)	Once a breach is detected, the organisation has 72hrs to determine the extent of the breach and to notify those affected. Detecting the breach can be harder than identifying affected data inside a datacentre, but privacy related data on a laptop can very problematic	Backups and archived files and emails can be content indexed to create a single searchable pool of high value information. This allows compliance and legal stakeholders to begin searching the content on assets known to have been breached (inc. laptops) to assist with the mandatory breach notification process.
Data minimisation principle (Article 25)	Organisations need to think differently about why, how and when data is copied; this includes dev & test, resilience backups, content analytics and other use cases.	Consolidating backup, archiving, analysis and information governance operations under Commvault dramatically simplifies data copy management. Policies can also be used to manage other functions such as Dev & Test
Defining use cases and managing consent (Article 6)	Data Protection Officers should be involved in data use case designs, and businesses need to be clear about how consent is achieved, what the scope is and retain proof	Defining use cases and managing consent are business process decisions. However, Commvault software can leverage its Search tools to locate consent linked to users, and manage retention by content or suitable tags
Data transfers (Articles 44-50)	An individual has the right to request that relevant, in scope data is collected and made available to new supplier, so that the new supplier can service their needs effectively	Using Commvault's compliance tools, unstructured data containing references to an individuals personal data can be located, collected and removed as required. Data in common apps can also be located, all from a single Search.
Data portability (Article 20)	When an individual requests a data transfer (as above) the new supplier must be provided with the relevant data in industry standard format so it can be used effectively.	When data is located, it can be collected and processed as required, then exported (data in common business applications can be located, but the application must do the export)



Simplify GDPR Processes Accelerate Cloud Adoption

SINGLE POINT FOR SEARCH, REPORTING & MANAGEMENT ON-PREMISES, PUBLIC CLOUD & SAAS

1 Data Protection Impact Assessment
2 PCI: Payment Card Industry, PII: Personally Identifiable Information
3 Right To Be Forgotten

Build a foundation for GDPR compliance now with a centralized approach to data management and retention. Find out more at commvau.lt/2qStBAH.

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM