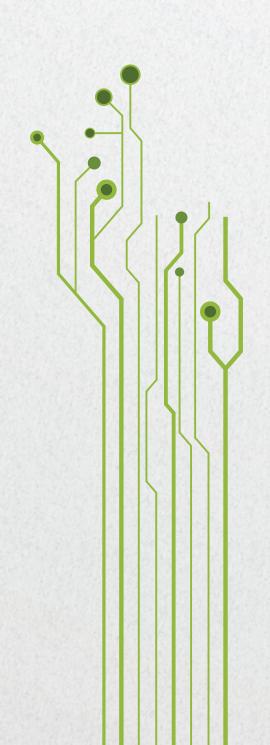


GDPR and Carbonite

How we support compliance with the EU's new General Data Protection Regulation (GDPR)



Carbonite hired privacy and cybersecurity experts at Dentons, an international law firm, to consult on the GDPR. This white paper summarises the requirements of the new law and the effects on organisations covered under the law, and explains how Carbonite products can support certain GDPR requirements. Statements made in this white paper about product functionality assume that the user has configured the product as recommended by Carbonite in User Guides and other supporting documentation.

On 25 May 2018, the GDPR will apply across all European Economic Area member states. It replaces and expands upon the existing EU Data Protection Directive. The new law allows authorities to impose fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher) for material breaches of the GDPR. It also requires that companies have appropriate data security in place to protect personal data, ensure the processes used to handle data are transparent, and are able to demonstrate compliance and accountability regarding data privacy governance.



What and whom does the law cover?

The GDPR defines "Personal Data" as any information that relates to an identified or identifiable natural person. This broad definition includes names and addresses, contact details, HR records and other identifiers such as device IDs, IP addresses, cookies, RFID tags and location data. Any organisation established in the EU that processes personal data must comply with the GDPR. Even having a subsidiary, branch, representative or agent in the area may be considered "establishment" under the law. It also applies to organisations not established in Europe that offer goods or services to individuals in Europe, regardless of whether payment is involved. Any organisation that monitors the behaviour of individuals located in Europe is also subject to the GDPR.

The law defines two distinct roles: controllers and processors. A controller is the entity that determines how personal data is handled—either on its own behalf or by processors it may engage. A processor is anyone hired by another entity to handle data. If you're a vendor or service provider, the former is likely your customer while the latter is you.

In a significant change from existing data protection law, under the GDPR, processors will have direct statutory obligations in relation to personal data being processed.

The GDPR defines processing as:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Service providers engaged in the following could be considered processors:

- CRM solutions
- Cloud storage or disaster recovery
- HR outsourcing

Controllers are obligated to use only processors that provide sufficient guarantees and appropriate security when processing personal data.

Rights and responsibilities

The GDPR codifies the rights of individuals whose personal data is being collected, as well as the responsibilities of controllers and processors to ensure personal data receives the appropriate level of protection. The law grants individuals whose data is subject to collection or processing additional rights compared with existing legislation, including the right to the following:

- 1. Data rectification
- 2. Erasure
- 3. Data portability

If personal data is inaccurate or incomplete, individuals have the right to have their data rectified or completed by the controller, free of charge and within a month, in most cases. Individuals can also request that their personal data be erased, including where continuing to process or hold the data is no longer relevant or appropriate. They can also require controllers to provide certain personal data about them in a portable or machine-readable format.

What were traditionally considered best practices in data governance are now expressly required by GDPR. Organisations must adhere to two key principles laid out in the text of the legislation:

Privacy by design – Controllers and processors must ensure data processing operations use appropriate technical and security measures to protect the privacy of personal data. This includes adopting data security and minimisation technologies such as encryption and pseudonymisation for both existing and new processing.

Privacy by default – Covered entities must ensure that, as a default, only personal data that is necessary for the specific purpose of the processing is processed. For example, access to data should be limited to those who need it for legitimate business purposes.

In the event of personal data breach (i.e., anything that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data), the GDPR requires controllers to notify regulators within 72 hours of discovery. The law requires processors to notify controllers without undue delay after becoming aware of a personal data breach.

Organisations are also required to keep records of their data processing activities, similar to the regulatory registrations currently required in certain EU jurisdictions. This applies to all controllers and processors that employ more than 250 people. Controllers and processors are required to test and audit against these standards regularly in order to demonstrate compliance.

How Carbonite supports GDPR compliance

Carbonite offers several plans that are engineered to support compliance with the GDPR. Our platform includes technology solutions for keeping personal data secure, ensuring data recency and restricting access for unauthorised users.

Carbonite Cloud Backup Powered by EVault

Rectification

Our server backup solutions are designed to automatically capture any and all changes made to source data. So, if you're correcting or supplementing data in production, those changes will be reflected in the next periodic backup without you having to do anything.

Erasure

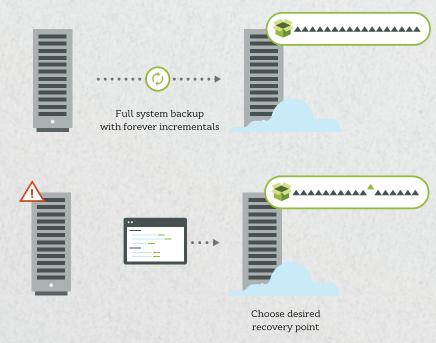
Data retention periods are easily configurable to wipe old datasets after a predetermined period. So, if you set retention periods for 30 days, any old backups would be deleted at the end of that period.

Privacy

Our solution separates the administrative portal from encryption keys, ensuring that if the admin credentials are compromised, customer data isn't at risk. Additionally, when the solution is configured properly, encryption keys are held by the customer, not by the service provider, which further limits access to data. The encryption used is AES-256, with one key per customer, ensuring accessing one key will not compromise all the data.

Records of processing

To assist with data processing record-keeping requirements, system logs can be used to show what's been backed up and what's been purged.



Carbonite Availability Powered by DoubleTake

Rectification

Carbonite Availability uses byte-level replication to capture changes in production in real time. Any corrections or deletions at the source are immediately reflected in the protection environment.

Erasure

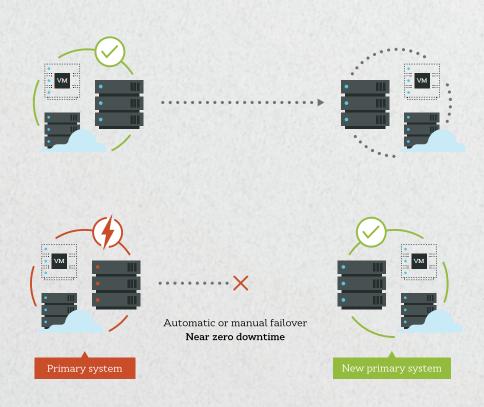
Snapshots that contain deleted data can be removed using the Carbonite Replication Console, or automatic pruning can be configured using Microsoft VSS.

Privacy

To ensure the privacy of data, Carbonite Availability uses AES encryption for data transmission. Security and access are managed through the use of security roles, with separate access privileges for both administrators and monitors. Replication of data is only possible for members of the local administrators security group for both the source and the target.

Records of processing

To assist with data processing record-keeping requirements, Carbonite Availability logs activities related to the operation of Carbonite Availability components, including logs for the management service, servers, jobs and the console. Since the components are transparent to the data layer, we minimize the personal data logged by design and by default.



Carbonite Endpoint Protection

Rectification

Carbonite Endpoint Protection automates the task of rectifying changes to information in the backup dataset by looking for changes on the protected device at predetermined intervals (every 15 minutes by default).

Erasure

Retention is configurable to preserve as many (or as few) versions of files as required. There's also the option to purge specific files from the vault. This allows users to manage archives on a file-by-file basis rather than backup-by-backup basis.

Privacy

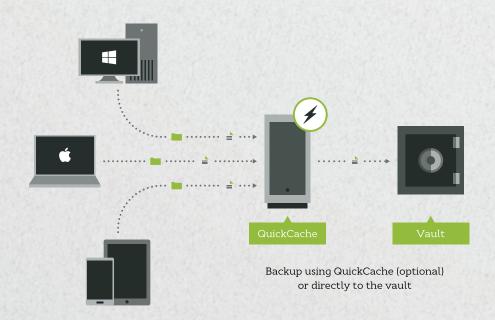
Carbonite Endpoint Protection performs global data deduplication on encrypted data. As a result, all data is encrypted on the endpoint before being backed up and stored in an encrypted state in the vault at all times. IT departments can maintain the master encryption keys on their own premises, independent of the vault location. Additionally, users and their access privileges can be deleted from the secure vault as needed.

Portability

To facilitate data portability, Carbonite Endpoint Protection allows administrators to isolate and restore backup datasets for a single end user. Recovered files can be easily ported to other storage, backup or archival environments.

Records of processing

Carbonite Endpoint Protection maintains an audit trail of administrator actions and mobile or web restore requests.



MailStore

Erasure

MailStore allows you to create global retention policies to ensure personal data is archived for only the period of time necessary to fulfill legal obligations or business needs. MailStore's advanced search can also help you fulfill erasure requests.

Privacy

MailStore uses advanced encryption to ensure the privacy of personal data contained in archived email messages, attachments, folders and user accounts.

Portability

The solution facilitates data portability by offering a simple path to exporting individual mailboxes securely and without restricting businesses to proprietary file formats.

Records of processing

MailStore uses an integrated auditing function to consistently log changes and events, which can be defined by the administrator.

Contact us for more information about how to use Carbonite to support compliance with the GDPR for your customers:

877-542-8637

DataProtectionSales@carbonite.com

This report is intended to provide general information only and is not intended to be relied on as a comprehensive guide or to provide legal or other advice. You should not take, or refrain from taking, action based on its content. Information contained in this report was obtained from third party law firms and/or public sources. No presentation or undertaking is made or given by any person as to the accuracy, completeness or reliability of this report or the information or views contained in this report. None of Carbonite, Dentons, or any of their respective partners, principals, employees, members, agents or contractors shall have any liability or obligation to any person arising from or in connection with any use, or misuse, or reproduction of this report or any information or views contained in this report. Neither Dentons nor Carbonite undertakes any responsibility to revise or update this report or otherwise to communicate to any person any inaccuracy in this report that is identified, whether as a result of new information, future events or otherwise.

GDPR requirement	Carbonite Cloud Backup Powered by EVault	Carbonite Availability Powered by DoubleTake	Carbonite Endpoint Protection	MailStore
Right to rectification	A fresh backup can account for any changes in the most current version of the backup.	Data that is changed on the production system is replicated to the target server in real time.	Changes would be reflected in the backup as files change within the primary system.	N/A
Right to erasure	Data retention periods are configurable by the service provider and customer.	Data that is deleted on the production system is deleted on the target system in real time.	Retention is configurable to preserve as many (or as few) versions of files as required.	Global retention helps ensure obsolete email data is wiped from the archive. Advanced search features let you crawl an entire email portfolio in a single step.
Right to data portability	N/A	N/A	Snapshots of specific end users' datasets can be easily ported to other storage, backup or archival environments.	Export individual mailboxes securely and without using proprietary file formats.
Records of processing	System logs show what's been backed up and what's been deleted in accordance with retention settings.	Logs of management service, server, job and console activity can be viewed within the central console.	An audit trail records all administrator actions and mobile or web restore requests.	An integrated auditing function logs changes and events, as defined by the administrator.

GDPR requirement	Carbonite Cloud Backup Powered by EVault	Carbonite Availability Powered by DoubleTake	Carbonite Endpoint Protection	MailStore
Privacy	When configured properly, advanced encryption, with one key per job, ensures accessing one key will not compromise all the data.	Encryption for data at rest is retained when replicated. An option is provided to encrypt data during replication.	All data is encrypted on the endpoint before being backed up, and is stored in an encrypted state in the vault at all times.	Advanced encryption ensures privacy of data contained in archived email messages, attachments, folders and user accounts.
Access	Administrative login credentials are kept apart from encryption keys, ensuring that if the admin credentials are compromised, customer data isn't at risk.	Administrators can configure two levels of privileges—one for secure roles and one for groups with the lowest necessary permissions.	Different permission levels are configurable to limit access when necessary.	By default, the administrator cannot access a user's archives. A special auditor user allows external auditors to access the archive.