Cloud Storage always encrypts your data on the server side (/storage/docs/encryption/default-keys), before it is written to disk, at no additional charge. Besides this standard behavior, there are additional ways to encrypt your data when using Cloud Storage. Below is a summary of the encryption options available to you:

- *Server-side encryption*: encryption that occurs after Cloud Storage receives your data, but before the data is written to disk and stored.
    - *Customer-supplied encryption keys* (/storage/docs/encryption/customer-supplied-keys): You can create and manage your own encryption keys for server-side encryption, which act as an additional encryption layer on top of the standard Cloud Storage encryption.
    - *Customer-managed encryption keys* (/storage/docs/encryption/customer-managed-keys): You can generate and manage your encryption keys using Cloud Key Management Service, which act as an additional encryption layer on top of the standard Cloud Storage encryption.
- *Client-side encryption* (/storage/docs/encryption/client-side-keys): encryption that occurs before data is sent to Cloud Storage. Such data arrives at Cloud Storage already encrypted but also undergoes server-side encryption.

ng: If you use customer-supplied encryption keys or client-side encryption, you must securely manage your keys and e that they are not lost. If you lose your keys, you are no longer able to read your data, and you continue to be charge e of your objects until you delete them.