This page discusses *client-side encryption*, which is any data encryption you perform prior to sending your data to Cloud Storage. For other encryption options, see Data Encryption Options (/storage/docs/encryption/).

When you perform client-side encryption, you must create and manage your own encryption keys, and you must use your own tools to encrypt data prior to sending it to Cloud Storage. Data that you encrypt on the client side arrives at Cloud Storage in an encrypted state, and Cloud Storage has no knowledge of the keys you used to encrypt the data.

When Cloud Storage receives your data, it is encrypted a second time. This second encryption is called *server-side encryption*, which Cloud Storage manages. When you retrieve your data, Cloud Storage removes the server-side layer of encryption, but you must decrypt the client-side layer yourself.

ng: Cloud Storage does not know if your data has already been encrypted on the client side, nor does Cloud Storage h
owledge of your client-side encryption keys. You must securely manage your client-side keys and ensure that they ar
you lose your keys, you are no longer able to read your data, and you continue to be charged for storage of your obje
ou delete them.