# Doctolib's Document Deletion

## Description

Doctolib is a European healthcare online service facility. It handles medical appointments between doctors and patients.

On Doctolib, it is possible to share documents, like prescription or result of lab testing, between the patient and his doctor. The documents are stored encrypted "with high level of confidentiality", on the patient online account server. It would be particularly relevant to have a guarantee that those confidential data have been erased upon request. It could even be mandatory for compliance with the European data protection law "GDPR" (General Data Protection Regulation), and its Article 17 known as the "Right to Erasure" or "Right to be Forgotten." It grants individuals the right to request the deletion or removal of their personal data by data controllers under certain circumstances.

Using Quantum certified deletion, it is possible for a user to store some data encrypted on a remote server, and at a later stage, request a mathematical proof that those data have been erased. After the proof was produced, the user has a guarantee that the plaintext cannot be recovered by the entity operating the server even if the original encryption key is revealed.

## Quantum advantage

There is a clear advantage in using a quantum information protocol as there is no classical solution for this problem. Indeed, it is always possible to make a copy of a classical ciphertext. An alternative solution would be under some circumstances to destroy the device physically.