Copycloud

General Data Protection Regulation (GDPR)

Introduction

GDPR, or the General Data Protection Regulation, is a set of privacy laws that were implemented in the European Union (EU) in 2018. It was designed to protect the personal data and privacy of EU citizens by giving them more control over their information.
Under GDPR, companies that collect, use, or store personal data must obtain explicit consent from the individual and provide them with clear information on how their data will be used.
The regulation also gives individuals the right to access, correct, or delete their personal data, as well as the right to object to its use for certain purposes.

Copycloud is a collaboration service that involves single/multiple parties working in a shared project. A shared project may have sensitive data, such as private documents, images, markdown files and more. As such, all documents must be protected in a way that complies with GDPR rules.

There are two main concerns about data security and distribution within the context of Copycloud:

1) User generated documents
2) User information and projects created by such user & what happens when they leave the application

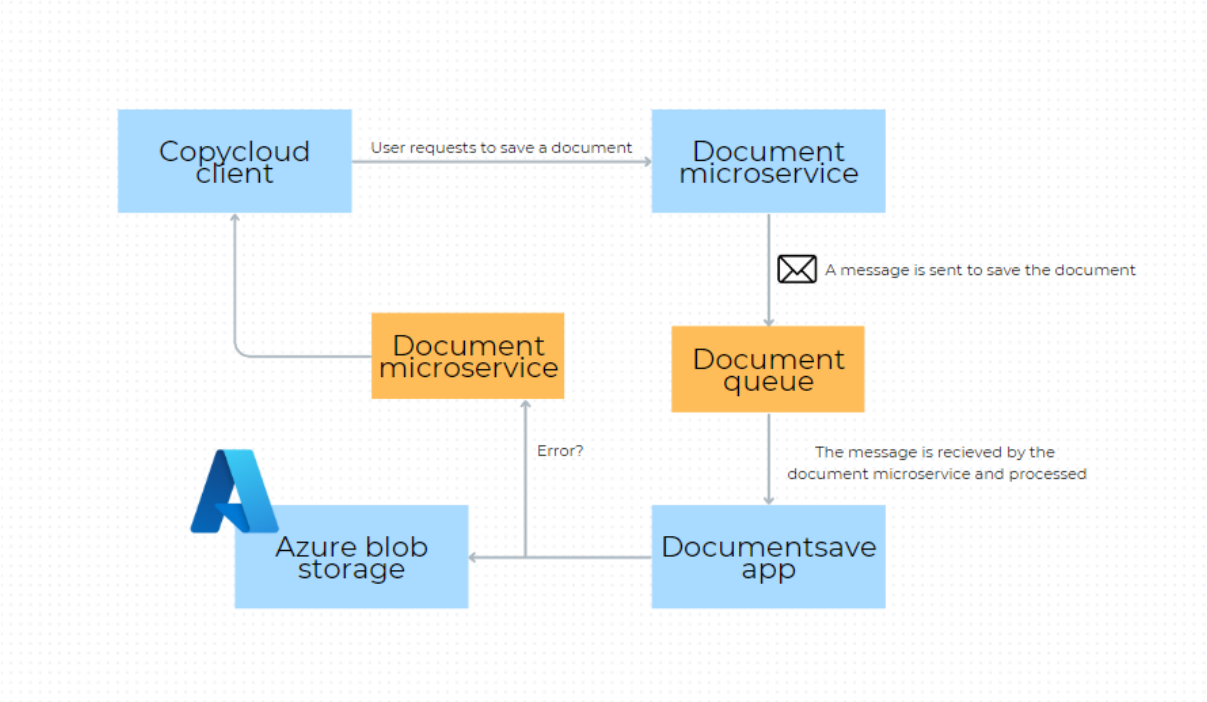
The following sections are dedicated to explaining each of the above mentioned concerns, as well as some additional things that are kept as a future note.

GDPR Data collection and documents

GDPR States that all data that is being collected must be stated in a public and legal manner. Having said this, Copycloud does not collect any hidden data about users. Furthermore, documents are server side encrypted both by Azure, as well as by Copycloud itself.

The below diagram shows how the underlying system of Copycloud works. This will help better understand the next sections of this document and clearly outline how GDPR is complied with.

Document saving Copycloud

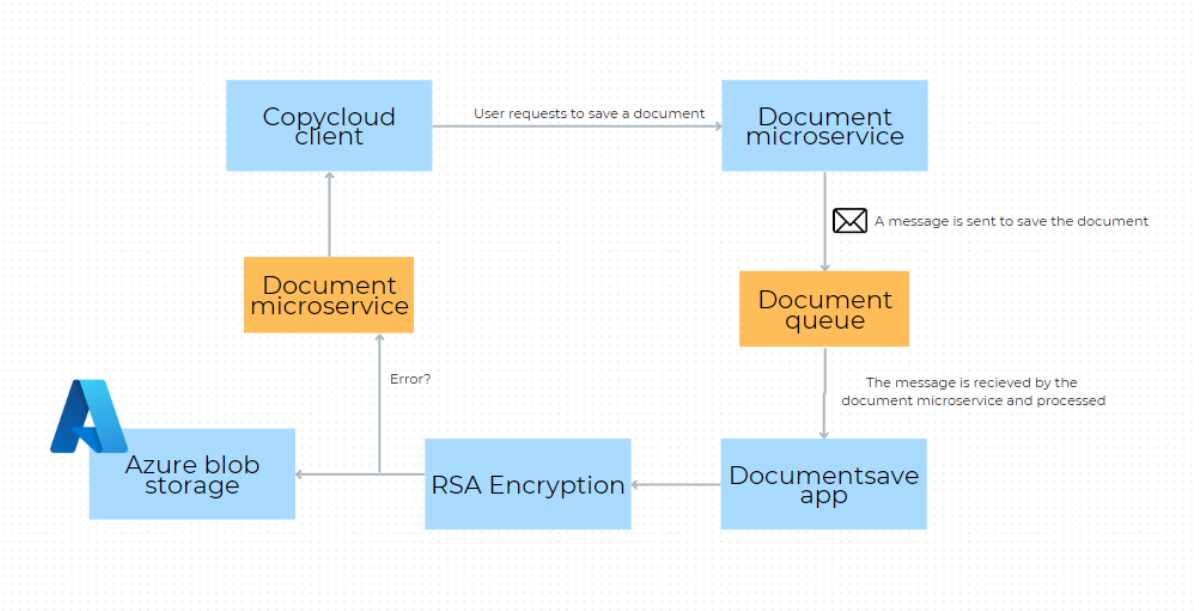


The system behind documents is based on event-driven architecture. This means that an event/message is sent that contains encrypted save data. This is then delegated to Azure blob storage for storing the data securely, as well as encrypting it.

For further reference, the following link goes into detail of why and how Azure blob storage complies with GDPR: https://github.com/sukykaur/AzureGDPR/blob/master/Azure%20Security%20and%20Compliance%20Blueprint%20-%20GDPR%20IaaS%20WebApp%20Overview.md

Nonetheless, in order to provide another layer of security and diminish any possibilities of Azure engineers to read any sensitive data generated by Copycloud users, the data is encrypted by Copycloud itself before being stored in Azure's blob storage containers.

Updated diagram for document saving



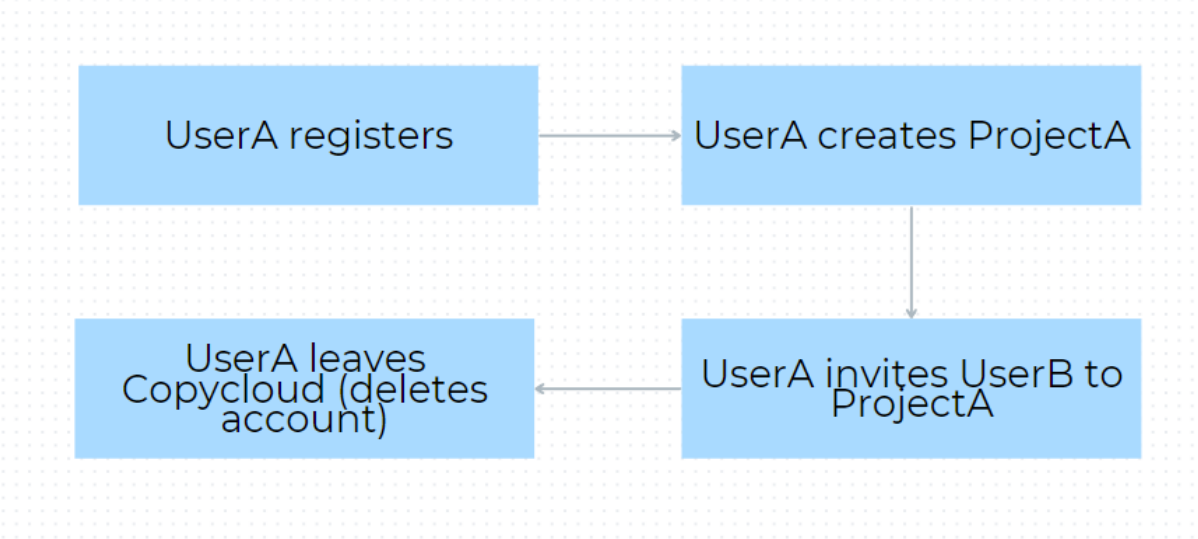
In the above updated diagram, we can see there's an intermediary step between storing into Azure's blob storage and making a request.

RSA is a widely used encryption algorithm that falls under the category of asymmetric encryption. It is named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is specifically designed for secure communication and confidentiality of information. In RSA, two different but mathematically related keys are used: a public key and a private key. The public key is openly shared and used for encryption, while the private key is kept secret and used for decryption.

What this means is that there's effectively a two layer of security, both by Azure and RSA which is the 2nd most used protocol for encryption.

User data and removal of users

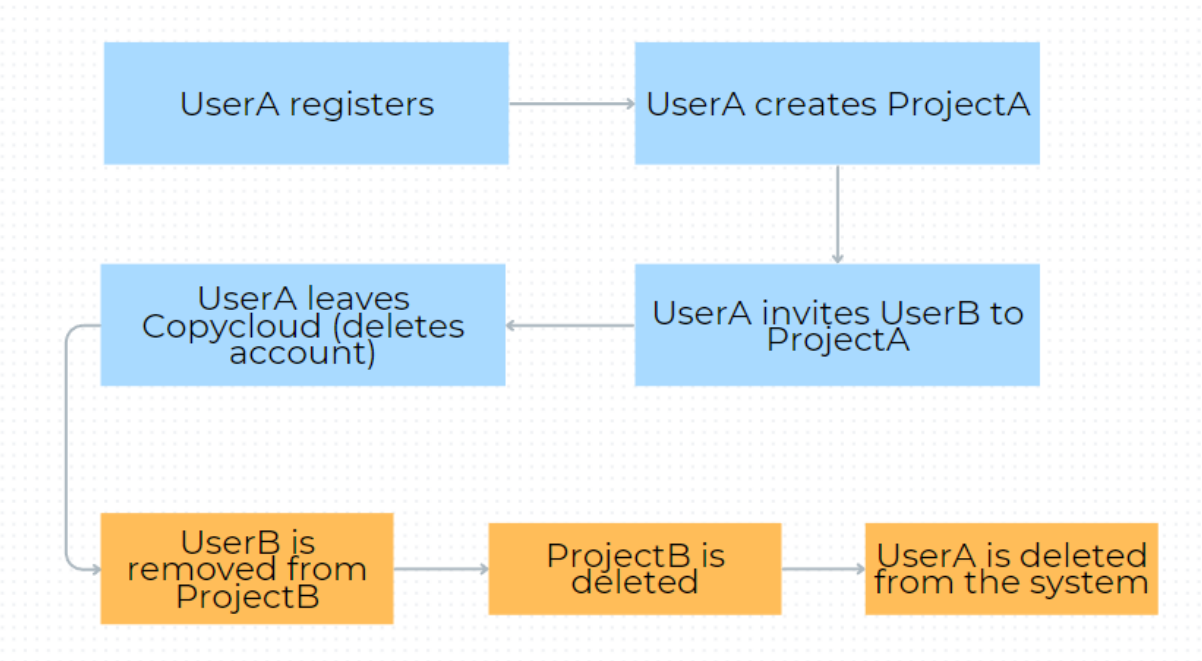
In order to best understand what needs to be taken into account when dealing with user data, it's best to begin by introducing a use case. This is represented under a diagram for easy demonstration.



The above shown diagram represents a case where a user registers, creates a sensitive document and invites another user to it. Finally, that same user decides to stop using Copycloud and deletes his account.

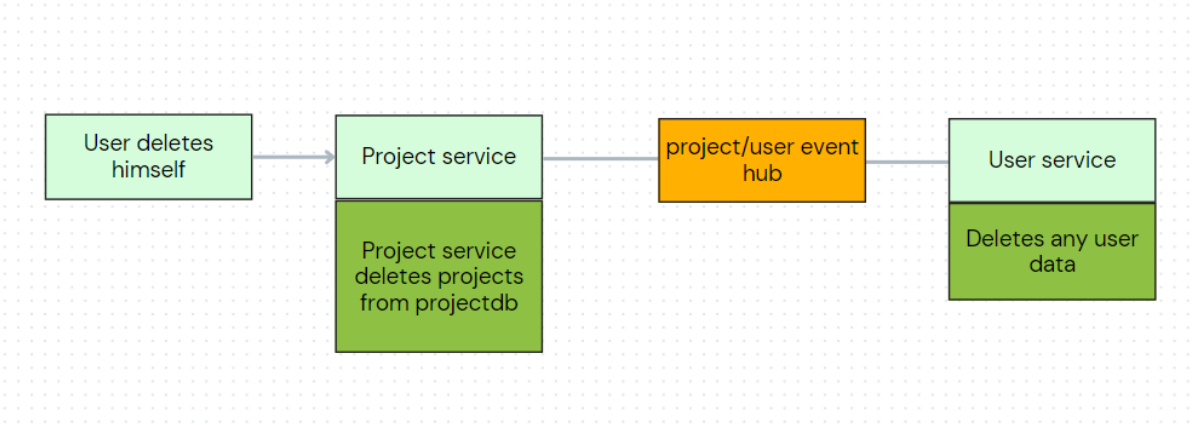
In this situation, since the user created the sensitive document, he is claimed as the original owner. Furthermore, because of how the underlying system of Copycloud works, each save/added content to each document can be easily tracked back.

In the case shown above, in order to comply with GDPR rules, once a user leaves and deletes his account, any sensitive data should be deleted. To visually demonstrate this process, a continuation of the diagram shown above can be seen on the next page.



Orange represents the extended process from the above shown diagram. What this means is that once a user decides to leave the application, both all of his data is deleted, as well as any trailing projects created by that user himself.

An actual overview of how the system does this in the background can be seen with the below diagram.



Conclusion

All of the processes and data obtained from users by Copycloud sits under all regulations and GDPR rules.

At this current state, Copycloud does not have any payment systems. However, if this changes in the future, Copycloud would have to follow regulations once again and store only relevant bank transfers/identifiers of users in the case of account deletion.