Fernet Encryption Algorithm

Reason for choosing Fernet

In this assignment, I have performed encryption of a file using the Fernet algorithm. It is an encryption algorithm in Python under cryptography module. Fernet is an asymmetric encryption technique. I used this method of encryption because the message being encrypted cannot be read or altered without the key. For the keys, it employs URL safe encoding and employs 128-bit AES in CBC mode, PKCS& padding, and HMAC with SHA256 authentication.

Would Fernet meet GDPR regulations?

Of course yes. The General Data and Protection Regulations is intended to protect the rights and data of individuals living in the European Union. Fernet meets GDPR regulations since is built by integrating a number of cryptographic primitives, it is ideal for encrypting data. A Fernet token is the end product of this type of encryption, and it provides a strong privacy and authenticity assurances. Data access is only through access using the key generated which is only available to the owner/user of the data.