# Data Protection and Protecting Sensitive Data

The General Data Protection Regulation (GDPR) states that data must only be collected and stored if it is necessary, as such when designing the project, a minimal amount of personal data is collected from the customer (Termly, n.d.). Due to this a customer only needs to enter their name, email, and password. A name is required as this allows a barber to know which customer is booking an appointment, the customers email is required as it enables a barber to contact a customer if needed for any reason. Finally, a customer’s password is needed to ensure that their account is secure and can only be accessed by them.

Since GDPR also states that a user has a right to request access to their data the user can access the details that are stored about them in the manage account page on the website (Termly, n.d.). This allows a user to review what is being stored in the database about them. This page also allows a user to change the data that is stored about them to ensure that it is up to date and correct which is abiding by another rule of GDPR.

The GDPR denotes sensitive personal data as the following: ethnic makeup, political stances, religious beliefs, trade union membership, health conditions, sexual orientation, and criminal files or court proceedings (GDPR Informer, 2017). The website that has been created does not store any data that relates to the listed sensitive personal data and therefore no precautions have been taken about storing sensitive personal data.

When a user is entering their password to the website it would be best practice to not store a password in the database directly, for security reasons. A proposed method of storing passwords is to store the hashed version of a password, this way the password that the user has entered is not stored anywhere and is protected as it can’t be accessed from the servers. When logging in to the website a user would enter their password into the password field, when pressing the submit button the entered password would be hashed and then compared to the stored hashed password that is on the database, if it is identical the user is then logged in to the website. This provides more security to the website for users.

Since the website handles payments, the decision was made to use a reputable payment gateway, PayPal, to ensure that customers data was secure when completing a transaction.

# References

GDPR Informer, 2017. *Sensitive Data and the GDPR: What You Need to Know.* [Online]   
Available at: https://gdprinformer.com/gdpr-articles/sensitive-data-gdpr-need-know#:~:text=Sensitive%20data%2C%20or%2C%20as%20the%20GDPR%20calls%20it%2C,information%20pertaining%20to%20one%E2%80%99s%20racial%20or%20ethnic%20makeup  
[Accessed 15 May 2022].

Termly, n.d. *What are the basic rules of the GDPR.* [Online]   
Available at: https://termly.io/faq/what-are-the-basic-rules-of-the-gdpr/#:~:text=Here%20are%20the%20basic%20rules%20of%20the%20GDPR%3A,for%20longer%20than%20is%20necessary.%20More%20items...%20  
[Accessed 14 May 2022].