Non-functional Requirements - Security

# Requirements

## User information should be stored securely

User information should be encrypted, and passwords should be hashed. This is to prevent leaking information in case of a data breach.

## Only required user information should be stored

By minimizing the information, we store and collect we would decrease the amount of information which could potentially be stolen in case of a data breach. It would also decrease the costs, as we would have to store less information.

## We should only be able to access the user’s information with the user’s permission

To prevent information being leaked by employees we should limit the amount of people who can access the user information, and/or to require the user’s permission to access and/or modify their information.

## We should explain to the user what information we collect

According to the GDPR and The Data Protection Act the user has the right to know what information we collect, which is why we should explain to them what information we collect, and how it is being used.

## We should give the user an option to opt out of us collecting the information

According to the GDPR and The Data Protection Act the user should always have the right to opt out of information collection. This would be a good idea regardless, as collecting less information means less information could be leaked/stolen.

## We should give the user an option to view and delete all their information, but only after making sure that they intend to do so.

According to the GDPR and The Data Protection Act the user has the right to request the deletion of all of their information, and we would have to comply with said request. We should always confirm that this is what the user wants us to do, as once the information is deleted, we will not be able to bring it back.

## The user information should not be kept for longer than necessary

According to the GDPR and The Data Protection Act the user’s information should only be kept for as long as we need it and should be deleted afterwards. This is also good practice regardless of these laws, as it means that the temporary information would not be able to be stolen once it has been deleted.

## The user should only be allowed to access their information

The users should not be able to access the private information of other users.

## We should store several backups of the information in a secure way. These backups should be encrypted to prevent them from being misused, and only authorized personnel should be able to decrypt them.

To prevent malicious actors from deleting the information we should store backups of the user information in a secure way.

# References

Intersoft Consulting (2016). *General data protection regulation (GDPR)*. [online] General Data Protection Regulation (GDPR). Available at: <https://gdpr-info.eu/>.

‌GOV.UK (2018). *Data Protection Act*. [online] GOV.UK. Available at: <https://www.gov.uk/data-protection>.

Wikipedia Contributors (2019). *Backup*. [online] Wikipedia. Available at: <https://en.wikipedia.org/wiki/Backup>.