CT255 Assignment 1  
GDPR  
Maxwell Maia  
21236277

Problem 1

GDPR and motivation

GPPR is the General Data Protection Regulation. It is a regulation that imposed obligations to any organization that targets or collects data related to people living in the European Economic Area. As of the 25th of May 2018, organizations could receive harsh fines of up to tens of millions of euros for violating its policies.

The main reason that GDPR was implemented is to harmonise the data privacy laws across the European Economic Area. This simplifies the regulatory environment for international business. This means that businesses and organisations won’t have to adopt a different data protection law for every region in the EEA. Now there are less obstacles to operate within the EU while being a data safe company. This encourages companies to do business within the EU.

GDPR has also brought strict rules for companies to follow that give rights to data subjects with regard to how their data is being used. This aims to reduce the amount of damage and the severity of damage done by data breaches.

More and more people are using online services and with many governmental organizations also transitioning to processing data digitally it has become increasingly important to keep data secure. Higher volumes of data are being processed and more sensitive data is being processed than ever before. This data can be a huge target for cyber criminals who are looking to gain access to bank accounts and personal information. Stolen data can also be kept at a ransom.

GDPR is, therefore, important to harmonise the data privacy laws and protect people’s valuable data.

Problem 2

Case study. An app/website used to keep in touch after graduation.

When a potential user of this app is to upload personal data, the company needs to store this data. According to GDPR laws, this counts as the processing of personal data, even if the data is only stored. Therefore, this company intends to provide a service that involves the obtaining, storing, transmitting and perhaps erasing of personal data. If this app is made available to people living in the European Economic Area, the company will need to comply with GDPR by law. This includes adhering to the GDPR’s key principles.

Key principles:

Fairness and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality

Accountability

The personal data being stored

Address  
Employment history  
Current position  
Salary range.

How the personal data should be treated with regards to the key principles  
  
This data is intended to only be shared with their former classmates however in the event of a data breach anyone could see this data. The users should be in control of their data. Steps need to be taken to secure this data and satisfy GDPR.

The company needs lawful basis to collect and use personal data (lawfulness). In this case the data requested will be collected and processed under consent. The company will need to clearly ask the user for consent to collect and use their data for the user uploads any personal information.

Everything that the company intends to use the data for must be clearly stated to the user when their consent is requested (fairness and transparency). This must also be a fair use of the data. It would be unfair if the company said that they wanted to sell this data to scam artists, for example.

A data protection notice must be given to the user. This will entail the identity and contact details of the following people that the company must employ/contract: the data controller, the data protection officer. This notice must contain other information regarding the access and retention of the data that the user is giving the company.

The purpose of the use of data must be clear and this purpose must be recorded (purpose limitation). The purpose here would be to collect, store and information and share it to former classmates.

The company should not ask for any more data than is necessary to perform this task (data minimisation). It wouldn’t be allowed to collect data about the user’s family member, for example. This is unnecessary because it does not help the company deliver the service that it has offered the user which is sharing your data to your former classmates.

The company should try to keep this stored data accurate. They can remind the user to update their details every year.

Data should not be kept for longer than needed. A retention period needs to be set for the personal data collected.

The company will need to document many aspects with regards to the security of this data under their use, and will be held accountable for failing to comply.

Personal data should be processed by means of “appropriate technical and organisational measures.” When the website / app is sending and retrieving information, the website / app can use encryption to uphold this principle of security.

References

GDPR.eu. 2022. *What is GDPR, the EU’s new data protection law? - GDPR.eu*. [online] Available at: <https://gdpr.eu/what-is-gdpr/> [Accessed 28 September 2022].

Nast, C., 2022. *What is GDPR? The summary guide to GDPR compliance in the UK*. [online] WIRED UK. Available at: <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018> [Accessed 28 September 2022].