Next Generation Technologies Assignment 1: GDPR

**Problem 1(>200 words):**

1. **What is GDPR?**

GDPR stands for General Data Protection Regulation. It is a binding regulation in EU law on data protection in the EU and the European Economic Area (EEA) and the transfer of personal data by EU residents outside of the EU and EEA, it was enforced in May 2018. GDPR strengthens the control and rights of personal data and simplifies the regulatory environment for international business. The regulatory contains provisions and requirements related to the processing of personal data of individuals who are located in the EEA and it applies to any enterprise regardless of its location and the data subjects’ citizenship or residence that is processing the personal information of individuals inside the EEA.

1. **Why was it introduced i.e motivations for this legislation**

The motivations for this legislation is to provide a set of standardised data protection laws across the EEA. This makes it easier for people to understand how their data is being used. GDPR improves the protection of European data subjects’ rights and clarifies what companies that process personal data must do to safeguard these rights which means companies and organisations competently ensure the security and protection of data held within the organisation. GDPR aims to regulate the processing of personal data of individuals in the EEA, it’s three primary concepts are transparency, compliance and punishment.

**Problem 2(>200 words):**

**A company develops a website and app that allows the users (i.e. the alumni of a given  
university course) to keep in touch after graduation.**

**Participants upload their personal data (e.g. address, employment history, current  
position, salary range, etc.) into the company’s database, from where it can be shared  
with / viewed by their former classmates (and them only!).**

**What are your thoughts / concerns with regard to GDPR compliance and the GDPR key  
principles? Your answer should be > 200 words.**

This company aims to develop a website to allow past college classmates to stay in touch with each other. They must comply with GDPR and follow the key principals to ensure all data collected on a lawful basis will be safely managed. Data must be necessary, proportionate, relevant, adequate, accurate, timely, and secure. Under

1. Lawfulness: this company must identify legal justification under GDPR for processing personal data. At least one of the following must apply when asking for personal data

* Consent
* Necessary for the performance of a contract
* Necessary for compliance with a legal obligation
* Necessary to protect the vital interests of the data subject or another person
* Necessary for the performance of a task carried out in the public interest
* Necessary for the purpose of the legitimate interests

The data this company is looking to share to former classmates can be classed as personal data (address, salary range etc). They must receive consent and justify their reasoning behind needing this data to the data subjects’. I don’t believe this company has lawful reasons for needing this data for this app. It is very unnecessary information with regards to an app looking to keep fellow classmates in contact.

1. Fairness and Transparency: personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject. The company must be clear and honest as to how they will process their data using the Data Protection Notice. They should clearly state it will only be shared to their classmates and not third party organisations.
2. Purpose limitation: the company must be clear about what the purpose of processing the data and record them as part of the documentation obligations. I feel the data required should be reconsidered for example the address and salary range, these are too personal to be shared and quite unnecessary in my opinion.
3. Data minimisation: personal data must be adequate, relevant and limited. This company must ensure they are not holding more data than needed which could make data subjects reject their terms and conditions leading to loss of subjects’. Focus on data that suits purpose of app such as occupation and not salary range and where you live should be optional to share, and in more of a broad sense like ‘city’, avoid sharing full address.
4. Accuracy: the company should ensure personal data is not incorrect or misleading and kept updated. It could be common that people try lie about data in order to portray a better life to feel better than their past classmates.
5. Storage limitation: the company must not keep the data collected for longer than it is needed and for good reason. If data subjects’ opt out of the app their data must be removed along with it as it is personal data.
6. Accountability and Governance: the company must have data controllers in order to meet the requirements of accountability.
7. Integrity and confidentiality: it is up to the company to process personal data securely by means of appropriate technical and organisational measures. They should consider risk analysis, organisational policies and physical and technical measures. I would suggest using pseudonymisation and encryption where necessary.