**In Class Assignment- Regulations for Data Privacy**

**Part 1**: **List of data privacy related issues that need to be regulated by the government** according to us-

* Data Collection: Regulate that only necessary data is collected and ensure responsible use.
* Personal Data Management: Requiring organizations to conduct privacy impact assessments for new technologies, systems, or processes that involve the collection or processing of personal data, assessing potential privacy risks and implementing necessary safeguards.
* Transparency of Data Usage: Ensure users are informed about how their data is shared/used.
* Data Portability: Enable individuals to easily move their data between service providers.
* Third-Party Selling of Data by Apps: Restrict unauthorized sale or transfer of personal data by apps.
* Location of Data Storage: Establish guidelines for data storage, whether on servers or users' devices.
* Opt-Out Options: accessible opt-out mechanisms for users who wish to withdraw consent.
* Parental Consent and Age-Appropriate Privacy Measures: Enforce consent requirements and age-specific privacy safeguards.
* Online Behavior Tracking: Mandate explicit user consent for tracking online activities.
* Security and Data Breach: Response to data breaches promptly and notifying affected individuals immediately should be regulated.

**Part 2:** **Choose one issue in particular** - Third Party Selling of data by apps

**Proposed Regulation**: Prohibition of Unauthorized Third-Party Selling of Personal Data

**Description:** App developers and service providers shall be prohibited from selling or transferring users' personal data to third parties without explicit consent from the users.

**How would we enforce it**- Following out proposed ways to enforce this regulation-

* Consent Verification: App developers must obtain clear and informed consent from users before collecting or sharing their personal data with third parties. Consent mechanisms should be user-friendly, transparent, and easily revocable.
* Audits and Compliance Checks: Government regulatory bodies would conduct regular audits and compliance checks on app developers and service providers to ensure adherence to the regulation. This would involve reviewing data usage policies, consent mechanisms, and any data sharing agreements.
* User Complaints and Reporting Mechanisms: Establishing channels for users to report potential violations or concerns regarding the unauthorized selling of their personal data. These reports would be investigated, and appropriate action would be taken against the violating companies.
* Public education: Government regulatory bodies can help to educate the public about the regulation and their rights under it. This would help to empower users to hold app developers and service providers accountable for their data practices

**What would be the consequence if a company violates the regulation?-**

* Financial Penalties: Companies found in violation of the regulation would face significant financial penalties proportionate to the severity of the violation and the size of the company.
* Suspension or Revocation of App Licenses: Repeated or severe violations may result in the suspension or revocation of the app developer's license, preventing them from distributing or operating their apps.
* Public Disclosure: Violating companies may be required to publicly disclose the nature of the violation, the steps taken for remediation, and any ongoing corrective actions.

**Part 3 -** **Search the GDPR to see if they have similar regulations as what your group has proposed and identify which sections.**

Yes, the above mentioned regulations are covered in general data protection regulations.

Below are the following sections of the GDPR that are relevant:

* Article 6: This article sets out the legal bases for processing personal data. One of the legal bases is consent, which is what the proposed regulation would require for the unauthorized third-party selling of personal data by apps.
* Article 7: This article sets out the requirements for consent. Consent must be freely given, specific, informed, and unambiguous.
* Article 9: This article sets out the special categories of personal data, which are data that is more sensitive and requires additional protection. The unauthorized third-party selling of this type of data would be prohibited under the proposed regulation.
* Article 13: This article sets out the information that must be provided to individuals when their personal data is collected. This information would include the purpose for which the data is being collected, the identity of the controller, and the rights of the individual.
* Article 14: This article sets out the additional information that must be provided to individuals when their personal data is collected from other sources. This information would include the source of the data and the purpose for which it is being used.
* Article 15: This article gives individuals the right to access their personal data.
* Article 16: This article gives individuals the right to have their data erased.
* Article 25: This article requires companies to take appropriate technical and organizational measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction.
* Article 33: This article requires companies to notify data protection authorities within 72 hours of becoming aware of a data breach.
* Article 34: This article requires companies to notify individuals about data breaches if the breach is likely to result in a high risk to the rights and freedoms of individuals.
* Article 20: This article gives individuals the right to have their data transferred to another company in a structured, commonly used, and machine-readable format.
* Article 79: This article sets out the penalties that can be imposed for violations of the GDPR. These penalties can be up to €20 million or 4% of global annual turnover, whichever is greater.