**ENTREPRENEURSHIP AND PRODUCT DEVELOPMENT.**

**ASSIGNMENT TWO.**

**GROUP WORK.**

Elizabeth Nduta C026-01-0693/2020

Paul Maigwa C026-01-1793/2020

David Nduati C026-01-1274/2019

Brian Minjire C026-01-1339/2019

James Njuguna C026-01-0678/2020

**QUIZ 1;**

*Concerning specific sections of the acts, outline ways in which the acts can frustrate (or discourage) the starting of a new ICT startup business.*

1. **Data Protection Act of 2020:**

* Limitation of Privacy Rights: Section 6 of the Act allows for the limitation of the right to privacy under Article 31 of the Constitution for purposes such as national security, prevention of crime, public interest, and compliance with law. This could discourage startup companies if they wish to deal with private information. For example, a platform advertised as safe and end-to-end encrypted.
* Quality of Information: Section 8 mandates that agencies ensure the data they collect is complete, accurate, up-to-date, and not misleading. This could also impose additional compliance burdens on startups.
* Collection of Personal Data: Section 7 requires agencies to collect personal data directly from the data subject for a specific, explicitly defined, and lawful purpose. This could impose additional compliance burdens on startups. An example is if a start-up needs to collect user data to give them targeted ads.
* Rights of Data Subjects: Section 9 grants data subjects rights to access, object to, correct, and delete their data. This could require startups to implement additional processes and systems to manage these rights which may increase their startup costs.
* Duty to Notify: Section 10 requires agencies to inform the data subject about the collection, purpose, intended recipients, and other relevant information before collecting personal data which could increase administrative overhead for startups and additional processes.
* Prohibition on Processing of Special Information: Section 24 prohibits the processing of special personal information unless certain conditions are met which could limit the types of data startups can collect and use.
* Retention of Information: Section 19 restricts the retention of personal data to the period necessary for achieving the purpose for which it was collected which could limit the ability of startups to use data for long-term analysis and strategic planning.
* Commercial Use of Data: Section 21 restricts the commercial use of personal data without express consent from the data subject or authorization under another law which could limit startups' ability to monetize their data-driven services.
* Protection and Security of Personal Data: Section 15 requires agencies to take reasonable steps to protect personal data from loss, damage, unauthorized access, and processing. This could require investment in security measures which may be costly.
* Notification of Security Compromises: Section 16 says agencies to notify the Commission and the data subject in case of unauthorized access or processing of personal data which could lead to reputational damage and legal consequences for startups.

1. **ICT Practitioner’s Act of 2018:**
2. **Professional Certification:**

* *Section*: *The requirement for certified ICT practitioners is primarily covered in Section 6 of the act.*
* The act emphasizes the importance of certified ICT practitioners. Start-ups may face challenges in hiring certified professionals due to limited budgets or a lack of available talent.

1. **Code of Conduct:**

* *Section: The ethical standards for ICT practitioners are outlined in Section 7.*
* The act outlines ethical standards for ICT practitioners. Start-ups must ensure their practices align with these standards, which can be restrictive or require adjustments.

1. **Liability for Practitioners:**

* *Section: The liability of practitioners is discussed in Section 8.*
* ICT practitioners can be held liable for professional negligence. Start-ups need to be cautious when providing services to clients to avoid legal repercussions.

1. **Regulatory Compliance:**

* *Section: The ongoing compliance requirements are implied throughout the act, particularly in sections related to professional conduct and responsibilities.*
* The act requires adherence to professional standards, which may involve ongoing training and certifications. For start-ups, this can be an additional burden.

1. **Impact on Innovation:**

* *Section: While not explicitly stated, the act’s overall impact on innovation and risk-taking is a broader theme that runs through various sections.*
* Stricter regulations might discourage start-ups from experimenting with new technologies or unconventional approaches due to fear of non-compliance.

**QUIZ 2;**

*Discuss ways in which the above challenges can be addressed to enable a young person to start their own ICT business.*

1. **Data Protection Act of 2020:**

* Educating on Data Protection and Privacy Laws: Understanding the points of data protection laws is crucial. This includes learning about the rights of data subjects, the obligations of data controllers, and the specific requirements for data processing activities. Examples through workshops, online courses, and seminars that focus on data protection and privacy.
* Develop a Comprehensive Data Protection Policy: Developing a well-defined data protection policy that aligns with the requirements of the Act is necessary. This policy should outline how personal data will be collected, processed, stored, and protected.
* Implement Data Protection Measures: Implementing technical and organizational measures to protect personal data is essential. This includes using encryption for data, implementing access controls, and regularly updating and patching systems to mitigate vulnerabilities.
* Appoint a Data Protection Officer (DPO): For businesses that process or monitor data on a large scale, having a DPO who is responsible for data governance and ensuring compliance with the Act is beneficial. The DPO can provide expert guidance on data protection matters and help manage the complexities of compliance.
* Train Employees: Ensuring that employees are fully trained in the nuances of data privacy and security is crucial.
* Engage with Third-Party Vendors Carefully: When entrusting the processing of personal data to third-party vendors, it's important to vet them carefully and monitor their policies and activities to ensure they remain compliant with the Act.
* Prepare for Incident Response: This plan should outline the steps to be taken in the event of a data breach, including notification requirements under the act.
* Leverage Technology and Tools: Utilizing data loss prevention (DLP) tools and secure access service edge (SASE) models can help protect personal data and ensure compliance with the Act. These technologies can help prevent data loss and unauthorized access.

1. **ICT Practitioner’s Act of 2018:**
2. Professional Certification:

* Training Programs: Encourage young entrepreneurs to participate in certification programs. Some organizations offer discounted rates for start-ups.
* Networking: Connect with certified professionals who can mentor and guide start-ups.

1. Code of Conduct:

* Ethical Culture: Establish an ethical culture within the start-up. Lead by example and emphasize integrity.
* Regular Training: Conduct regular training sessions on ethical behaviour and professional conduct.

1. Liability for Practitioners:

* Insurance: Consider professional liability insurance. It provides financial protection in case of claims.
* Clear Contracts: Ensure contracts with clients clearly define responsibilities and limitations.

1. Regulatory Compliance:

* In-House Compliance Officer: Appoint someone responsible for monitoring compliance. It need not be a full-time role initially.
* Collaborate with Industry Bodies: Join industry associations that guide compliance.

1. Impact on Innovation:

* Balancing Act: Encourage start-ups to innovate while staying within legal boundaries.
* Pilot Projects: Test innovative ideas in smaller pilot projects before full-scale implementation.