SharkStriker

DATASHEET

Kenya Data Protection Act

1 | Overview of Kenya Data Protection Act

Data is an essential part of everyday business operations for many small, medium, and large businesses. Since these businesses store and exchange huge chunks of sensitive personal data (Personal Identifiable Information (PII)), it is critical to protect this data from cyber criminals who may exploit it for political or monetary motives. After the aftermath of cyber attacks that have left many customers and businesses devastated, the Kenyan government had to come up with an Act that safeguards the right to privacy of its citizens. This gave birth to Kenya Data Protection Act 2019. It is a comprehensive set of guidelines and regulations that governs the processing and storage of personal data by government and private authorities.

2 | What is Kenya Data Protection act?

The government of Kenya has stated in its constitution that the right to privacy is a fundamental right. Therefore, to protect this right, the government released the Data Protection Act under Article 31 (c) and Article 31 (d). It was put into effect on 25 November 2019 and was enacted in November 2020.

In 2021, the ICT Cabinet Secretary appointed a Task Force for the Development of the Data Protection General Regulations ('Taskforce'). The Task Force along with the Office of the Data Protection Commissioner (ODPC) published Data Protection Regulations (General Regulations) in 2021, Data Protection Regulations (Protection Registration of Data Controllers and Data Processors), Data Protection Regulations (Complaints Handling and Enforcement Procedures Regulations).

According to the Kenya Data Protection Act (KDPA) 2019, any organization from Kenya, collecting or storing Data of the residents of Kenya should abide by the KDPA. All kinds of sensitive personal data including:

1. Name
2. Identification Number
3. Account number
4. IP Address
5. Username
6. GPS coordinates
7. KRA Pin

| Sensitive information such as:

- Race
- Health
- Social Origin
- Biometric Data
- Property Details
- Marital Status

Failure to comply with obligations under KDPA may result in an Enforcement Notice from ODPC which contains a list of steps that are to be taken for remediation until a specified period.

| Punishment for violation:

Fines

- Maximum amount - KES 5 million or
- 1 percent of the annual turnover of the preceding financial year (whichever is lower)
- Up to KES 3 million for non-specific penalties
- Daily fines of up to KES 10,000 for identified breaches until rectification

Prison sentence

- Up to 2 years

3 | On whom is KDPA 2019 compliance applicable?

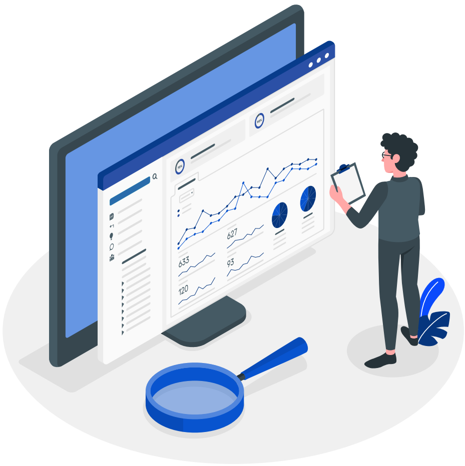
It applies to both resident and non resident of Kenya who are involved in data processing and control of Kenyan data.

4 | What SharkStriker Can Do for This Compliance?

- Data collection
- Data transfer
- Categorization of data that is to be collected
- Protection and security of the data collected
- Publication and disclosure of data
- Data Retention
- Accuracy of data collection
- Data updation
- Data Deletion

5 | What are the exemptions under this act?

- Processing of personal data relating to personal or household activity
- If publication of data is artistic or literary in nature
- Data controllers and processors are exempted from seeking consent in only specific circumstances such as - if data is subject to public interest or fulfillment of legal obligation or for performance of task given by any public authority.



6 | What aspects are not covered in this act?

- Data Governance
- Data Strategy
- Data Migration
- Data Warehousing
- Data Quality Checks
- Data Processing

7 | How can SharkStriker help you?

With a team of cybersecurity experts and compliance consultants, SharkStriker can provide you with extensive 360-degree compliance with KDPA 2019 through the following steps:

KDPA 2019 360 degree assessment:
This is the very first step that involves assessing all of your existing IT infrastructure to determine how compliant it is. This includes the Identification of assets, controls, gaps & risk assessment, and generation of compliance reports.

Roll out and implementation:
In this phase, we commence the implementation of solutions to treat risks and roll out a full-blown risk treatment plan. We implement security measures, and technology controls, and run training and awareness to mitigate human error. We deploy management control to mitigate risks, enhance physical security and prevent unauthorized access.

Security Services:
This phase is focused on the augmentation of the cybersecurity of your existing IT infrastructure through a range of cybersecurity services. These services include: Periodic VAPT (vulnerability assessment and penetration testing), Managed Network and Security (including firewall installation, configuration & management), Network Security Monitoring, Threat Detection and Response with SIEM, 24/7 monitoring, Incident Response, AI-based EDR, Cloud Security Assessment, and Monitoring.

Compliance Review:
In the final phase, we review and audit the level of implementation of the KDPA 2019 through: Information and Security Management Review (ISMS), Mock Audits for the identification of weak and exploitable ISMS points, KDPA 2019 Internal Audit, and seamless assistance with external audit for certification.

8 | Consequences of not complying with KDPA Compliance

Any form of violation of the KDPA compliance may attract penalties of up to KES 5 million or a prison sentence of 3 years or both. A daily fine of KES 10000 may also be imposed in the case of a listed breach until it is remediated.

9 | SharkStriker Compliance Services

SharkStriker provides the following KDPA compliance services:

Analysis of KDPA Compliance Gaps

We conduct a thorough gap analysis of the current infrastructure, looking for all the flaws and gaps in compliance.

Cyber Risk Treatment Plan

We assess the infrastructure of all the cyber risks and prepare a cyber risks treatment plan for remediation in accordance with the KDPA guidelines.

Policies & Procedures for KDPA

Based on the outcome of the risk and compliance gap assessment, we devise specific policies, procedures, and measures for KDPA compliance.

Data protection measures

Our skilled cybersecurity professionals take measures to secure all the digital data assets and implement various controls to prevent the most immediate cybersecurity threats and bad actors from gaining access to data.

Threat Intelligence

We ensure increased compliance through enhanced cybersecurity with intelligent threat hunting and knowledge base creation of threats for quicker identification and response.

Observance audits

Our cyber compliance consultants conduct an extensive audit of your infrastructure to scan it for noncompliance to KDPA 2019.

Risk Mitigation Plan

To prevent threats to data such as data theft, data breach, or data loss of any kind, SharkStrikers evaluates threats and creates mitigation plans to effectively prevent them from happening in the first place. .

Regular Updates

SharkStriker makes sure that your cybersecurity infrastructure remains up to date with security developments such that your IT infrastructure remains free of security flaws.

Security Checks

Data security and privacy are ensured through periodic security assessment and testing that ensure that your organization is compliant with KDPA 2019 at all times.

Review of KDPA implementation

Post KDPA implementation, we review the existing infrastructure of flaws in compliance and implement suitable measures to ensure complete compliance to KDPA 2019.

Internal Audit of KDPA

We conduct an in-depth internal audit of the infrastructure such that we can determine inherent flaws and prepare recommendations for its improvement.

Application of Technology

We deploy all the necessary technological tools and solutions that are stated in the guidelines of KDPA.

About SharkStriker

SharkStriker is a trailblazing cybersecurity services vendor with a mission to simplify cybersecurity for its partners across industries through its technologically driven human-led open architecture platform STRIEGO. It seeks to cater to some of the industry's most immediate challenges such as siloed cybersecurity, increasing cost of cybersecurity solutions, changing regulatory environment, and increasing reliance on multiple vendors for multiple aspects of cybersecurity and compliance.

With STRIEGO, SharkStriker is able to assist its network of partners and customers through effective augmentation of cybersecurity posture as per use cases, extending visibility, compliance management, and round-the-clock support for incident response.

Through a team of threat-striking experts, they have made their presence across MEA, North America, Europe, and Asia.

Globally recognized, Globally trusted.

Phone: +1 925 5321900
Email: sales@sharkstriker.com
Website: www.sharkstriker.com

SharkStriker