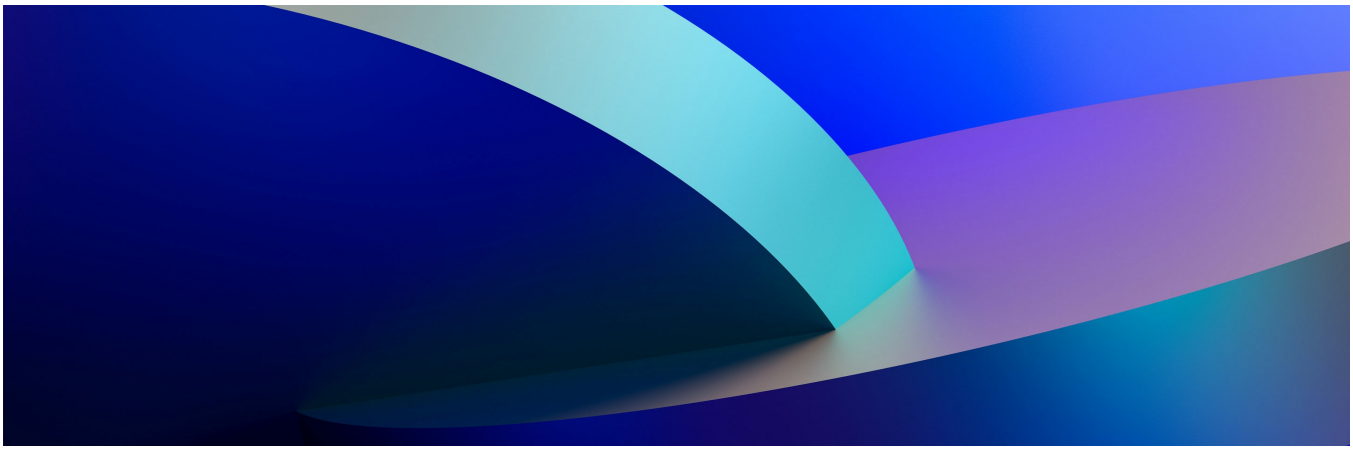

Data protection and cybersecurity laws in Kenya

Data protection

1. Local data protection laws and scope

Data protection in Kenya is regulated by the Data Protection Act No. 24 of 2019 (the "DPA").

The DPA came into effect on 25 November 2019.

Subsequently, the following regulations came into effect on 31 December 2021:

1. The Data Protection (General) Regulations, 2021;
2. The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021; and
3. The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021,

(the "**Regulations**").

The Data Protection Act No. 24 of 2019:
http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019/

The Data Protection (General) Regulations, 2021:
https://www.odpc.go.ke/download/data-protection-regulations/

The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021.

2. Data protection authority

The Office of the Data Commissioner.

The Data Commissioner was formally appointed on 16 November 2020.

3. Anticipated changes to local laws

We do not anticipate any further changes to the data protection laws in Kenya.

4. Sanctions & non-compliance

Administrative sanctions:

The DPA gives the Office of the Data Commissioner the power to impose administrative fines for failure to comply with the DPA.

The Office of the Data Commissioner may impose a fine of up to KES. 5 million (approx. USD. 50,000) or, in the case of an undertaking, up to 1% of its annual turnover of the preceding financial year, whichever is lower. The fine is payable to the Office of the Data Commissioner.

Failure to comply with an order of the Office of the Data Commissioner is considered an offence under the DPA.

Section 65 of the DPA accords all data subjects the right to compensation from data processors or controllers for damage caused to them.

Criminal sanctions:

There are certain specific offences under the DPA, including:

- Unlawful disclosure of personal data in a manner incompatible with the purpose for which the data was collected;
- Unlawful disclosure of personal data that the data processor processed without the prior authorisation of the data controller;
- Obtaining access to personal data without the prior authorisation of the data controller or processor holding the data;
- Disclosure of personal data to a third party without prior authorisation by the data controller or processor holding the data;
- Sale of personal data obtained unlawfully. Advertising the sale of such data constitutes an offer to sell under this offence;
- Failure to register with the Office of the Data Commissioner as a data processor or controller;
- Provision of false or misleading information during the application process for registration as a data processor or controller; and
- Obstruction of the Office of the Data Commissioner during an investigation.

On conviction, an offence under the DPA carries a general penalty of a fine not exceeding KES. 3 million (USD. 30,000) or an imprisonment term not exceeding ten years, or both. In addition, obstruction of the Data Commissioner during an investigation is an offence liable to a fine not exceeding KES. 5 million (USD. 50,000) or imprisonment for a term not exceeding two years, or to both.

5. Registration / notification / authorisation

The DPA requires all data processors or controllers to register with the Office of the Data Commissioner.
However, data processors and data controllers with an annual turnover of below KES. 5 million (approx. USD. 50,000) or annual revenue of below KES. 5 million (approx. USD. 50,000) and have less than 10 employees are exempt from the mandatory requirement for registration. This exemption does not apply to data controllers or data processors who process personal data for the following purposes:

- Canvassing political support among the electorate
- Crime prevention and prosecution of offenders
- Gambling
- Operating an educational institution
- Health administration and provision of patient care
- Hospitality industry firms (excluding tour guides)
- Property management, including the sale of land

- Provision of financial services
- Telecommunications networks or service providers
- Businesses that are wholly or mainly in direct marketing
- Transport service firms (including online passenger hailing applications)
- Businesses that process genetic data

To register as a data controller or data processor, the applicant must lodge with the Office of the Data Commissioner:

1. A duly filled application form;
2. Receipt for the prescribed registration fees;
3. A copy of the establishment or incorporation documents;
4. Particulars of the data controllers or data processors including name and contact details;
5. A description of the purpose for which personal data is processed; and
6. A description of categories of personal data being processed.

Once the application for registration is processed and approved, a Certificate of Registration will be issued, valid for 24 months from the date of issuance.

6. Main obligations and processing requirements

Data Processing Principles:

All data processors/controllers are required to follow the data protection principles, which are:

1. Data processing in accordance with the right to privacy of the data subject;
2. Fair and transparent processing of a data subject's personal data;
3. Collection of personal data for specified and legitimate purposes and not further processing beyond those purposes;
4. Purpose limitation for data collected;
5. Collection of personal data relating to family or private affairs only where a valid explanation is provided;
6. Accuracy of collected personal data and every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
7. Personal data is to be kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
8. Personal data shall not be transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject.

Duty to Notify:

Before collecting any personal data, data processors/controllers are required to notify a data subject of:

1. Their rights as data subjects under the DPA;
2. The fact that their data is being collected and the purpose for the collection;
3. Any third parties that have or will have access to their data, including details of safeguards adopted;
4. The contacts of the data controller/processor and any other entity receiving the collected personal data;
5. The technical and organisational security measures taken to ensure the integrity and confidentiality of the data;
6. Whether the data is being collected pursuant to any law and whether such collection is voluntary or mandatory; and

7. The consequences, if any, if they fail to provide all or any part of the requested data.

Lawful Processing:

Personal data may only be processed on the lawful basis provided under Section 30 of the DPA as:

1. Consent: the individual has given clear consent for a data processor or controller to process their personal data for a specific purpose;
2. Contract: the processing is necessary for a contract's performance between a data processor or controller and the data subject or because the data subject has asked the data processor or controller to take specific steps before entering into a contract;
3. Legal obligation: the processing is necessary for a data processor or controller to comply with the law (not including contractual obligations);
4. Vital interests: the processing is necessary to protect the vital interests of the data subject or another natural person;
5. Public task: the processing is necessary for a data processor or controller to perform a task in the public interest or the exercise of official authority vested in the controller;
6. Legitimate interests: the processing is necessary for a data processor or controller's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the data subject's data which overrides those legitimate interests; and
7. Historical, Statistical, Journalistic, Literature and Art or Scientific research: if the data is required in such pursuits.

Data Retention Obligations

Data processors and data controllers are required to retain personal data for a lawful purpose and only for as long as may reasonably be necessary for the purpose.

Under the Regulations, the data controllers and processors are required to establish a data retention schedule with appropriate time limits for review of the need for continued storage. Periodic audits of the data retained are also required.

Upon lapse of the purpose for which the personal data was collected, data controllers and data processors are required to erase, delete, anonymise or pseudonymise the personal data retained.

Obligation to Process Personal Data Anonymously or Pseudonymously

A data subject may request that their data be processed anonymously or pseudonymously.

Upon such a request, the data processor or data controller may accede to the request if the reason provided is that the data subject wishes:

1. not to be identified;
2. to avoid subsequent contact such as direct marketing from an entity or third parties;
3. to enhance their privacy on the whereabouts of a data subject;
4. to access services such as counselling or health services without it becoming known to others;
5. to express views in a public arena without being personally identified; or
6. to minimise the risk of identity fraud.

Data Sharing Obligations

A data controller or data processor may share or exchange personal data collected if requested in writing by another data controller, data processor, third party or a data subject.

The written request for data sharing must specify the purpose for which the personal data is required, the duration it will be retained, and proof of safeguards in place to secure the personal data.

Under the Regulations, upon such a request, the providing data controller or data processor is required to enter into a data-sharing agreement with the requesting party.

Automated Individual Decision Making in Data Processing

While permitted under the DPA and the Regulations, a data controller or data processor utilising automated individual decision making in their data processing is required to:

1. inform the data subject when engaging in processing based on automated individual decision making;
2. provide meaningful information about the logic involved in such processing;
3. ensure:
    1. specific transparency and fairness requirements are in place;
    2. rights for a data subject to oppose profiling and specifically profiling for marketing are present; and
    3. where the processing is likely to result in high-risk to the rights and freedoms of the data subject, a data protection impact assessment is carried out;
4. explain the significance and envisaged consequences of the processing;
5. ensure the prevention of errors;
6. use appropriate mathematical or statistical procedures;
7. put appropriate technical and organisational measures in place to correct inaccuracies and minimise the risk of errors;
8. process personal data in a way that eliminates discriminatory effects and bias; and
9. ensure that a data subject can obtain human intervention and express their point of view.

Data Protection Policy

Data processors and data controllers in Kenya are required to develop, publish and regularly update a policy reflecting their personal data handling practices.

Contracts of Data Controllers and Data Processors

Data processors and data controllers may only engage through a written contract. The written contract must provide specified particulars under the Regulations.

Data processors are not permitted to engage the services of a third party without the prior authorisation of the data controller. Once authorisation is given, the data processor shall enter into a contract with the third party.

Personal Data required to be specifically processed in Kenya

Data controllers and data processors processing personal data based on the grounds of strategic interests of the state are required to process such personal data through a server and data centre located in Kenya or store at least one serving copy of the concerned personal data in a data centre located in Kenya.

Elements in Implementing Data Protection by Design or Default

Data controllers and data processors are required under the Regulations to establish data protection mechanisms aligned with the DPA and the Regulations and design technical and organisational measures to safeguard and implement the data protection principles. These principles are spelt out in the Regulations, where the elements of the principles and the obligations of data controllers and data processors are listed as follows:

Lawfulness:

To implement this principle, the following elements are necessary:

- appropriate legal basis or legitimate interests clearly connected to the specific purpose of the processing;
- processing that is necessary for the purpose;
- the data subject is granted the highest degree of autonomy possible with respect to control over their personal data;
- a data subject knowing what they consented to and easy means to withdraw consent; and
- restricting processing where the legal basis or legitimate interests ceases to apply.

Transparency:

To implement this principle, the following elements are necessary:

- the use of clear, simple and plain language to communicate with a data subject for them to make decisions on the processing of their personal data;
- easily access to information about the processing of personal data of the data subject;
- access for the data subject to the information on the processing at the relevant time and in the appropriate form;
- the use of machine-readable language to facilitate and automate readability and clarity;
- providing a fair understanding of the expectation with regards to the processing, particularly for children or other vulnerable groups; and
- providing details of the use and disclosure of the personal data of a data subject.

Purpose Limitation:

To implement this principle, the following elements are necessary:

- specifying the purpose for each processing;
- determining the legitimate purposes for the processing of personal data before designing organisational measures and safeguards;
- the purpose for the processing being the determinant for personal data collected;
- ensuring a new purpose is compatible with the original purpose for which the data was collected;
- regularly reviewing whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation; and
- the use of technical measures, including hashing and cryptography, to limit the possibility of repurposing personal data.

Integrity, Confidentiality and Availability:

To implement this principle, the following elements are necessary:

- having an operative means of managing policies and procedures for information security;
- assessing the risks against the security of personal data and counter identified risks;
- processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;
- ensuring only authorised personnel have access to the data necessary for their processing tasks;
- securing transfers such that they are secured against unauthorised access and changes;
- securing data storage from unauthorised access and alterations;
- keeping back-ups and logs to the extent necessary for information security;
- using audit trails and event monitoring as a routine security control;
- protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;
- having in place routines and procedures to detect, handle, report, and learn from data breaches; and

- regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.

Data Minimisation:

To implement this principle, the following elements are necessary:

- avoiding the processing of personal data altogether when data processing is not necessary for the relevant purpose;
- limiting the amount of personal data collected to only what is necessary;
- maintaining an ability to demonstrate the relevance of the data to the processing in question;
- pseudonymising personal data as soon as it is no longer necessary to have directly identifiable personal data, pseudonymised data and identification keys stored separately;
- anonymising or deleting personal data where it is no longer necessary for the purpose;
- making data flow efficient to avoid the creation of more copies or entry points for data collection than is necessary; and
- the application of available and suitable technologies for data avoidance and minimisation.

Accuracy:

To implement this principle, the following elements are necessary:

- ensuring data sources are reliable in terms of data accuracy;
- having personal data particulars being accurate as necessary for the specified purposes;
- verification of the correctness of personal data with the data subject before and at different stages of the processing depending on the nature of the personal data, in relation to how often it may change;
- erasing or rectifying inaccurate data without delay;
- mitigating the effect of an accumulated error in the processing chain;
- giving data subjects an overview and easy access to personal data in order to control accuracy and rectify as needed;
- having personal data accurate at all stages of the processing and carrying out tests for accuracy at critical steps;
- updating personal data as necessary for the purpose; and
- the use of technological and organisational design features to decrease inaccuracy.

Storage Limitation:

To implement this principle, the following elements are necessary:

- having clear internal procedures for deletion;
- determining what data and length of storage of personal data that is necessary for the purpose;
- formulating internal retention statements implementing them;
- ensuring that it is not possible to re-identify anonymised data or recover deleted data and testing whether this is possible;
- the ability to justify why the period of storage is necessary for the purpose, and disclosing the rationale behind the retention period; and
- determining which personal data and length of storage is necessary for back-ups and logs.

Fairness:

To implement this principle, the following elements are necessary:

- granting the data subjects the highest degree of autonomy with respect to control over their personal data;

- enabling a data subject to communicate and exercise their rights;
- elimination of any discrimination against a data subject;
- guarding against the exploitation of the needs or vulnerabilities of a data subject; and
- incorporating human intervention to minimise biases that automated decision-making processes may create.

7. Data subject rights

1. Right to be informed of the use to which their personal data is to be put;
2. Right to access their personal data in the custody of the data controller or processor;
3. Right to object to the processing of all or part of their personal data;
4. Right to correction of false or misleading data;
5. Rights to deletion of false or misleading data about them;
6. Right to withdraw the consent given to data processor or controller at any time;
7. Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject;
8. Right to object to the processing of their personal data, unless the data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment, exercise or defence of a legal claim; and
9. Right to receive personal data concerning them in a structured, commonly used and machine-readable format and the right to transmit such data from one data controller to another.

8. Processing by third parties

The DPA does not prohibit the processing of personal data by third parties but requires that the data subject be informed of any third parties that may have access to their personal data and the safeguards adopted to ensure their data security.

The data processor or controller must also provide the third party's contact details to the data subject. This information should be provided before the data is collected.

9. Transfers out of country

Before a data controller or processor transfers data outside Kenya, they need to ascertain that the transfer is being done on one of the following bases:

1. Appropriate data protection safeguards

This basis may be relied on where:

- there is a legal instrument binding the foreign entity receiving the personal data equivalent to the protection under the DPA;
- the data controller has assessed all the circumstances surrounding transfers of the type of personal data to another country or international organisation and concluded that appropriate safeguards exist to protect that data.

2. An adequacy decision made by the Data Commissioner

An adequacy decision is a determination of the Data Commissioner that the other country or territory or one or more specified sectors within that other country or the international organisation ensures an adequate level of protection of personal data. To rely on this basis, the data controller would need to rely on an adequacy decision made by the Data Commissioner before any transfer can be made.

The Data Commissioner publishes the list of the countries, territories and specified sectors within that other country and relevant international organisations for which a decision has been made that an

adequate level of protection is ensured on the website of their office.

3. Transfer as a necessity

The transfer out of Kenya would be considered out of necessity if it is necessary:

- for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;
- for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
- for any matter of public interest;
- for the establishment, exercise or defence of a legal claim;
- to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
- for compelling legitimate interests pursued by the data controller or data processor, which are not overridden by the data subjects' interests, rights, and freedoms.

4. Consent of the data subject

To rely on this basis for the transfer of the data out of Kenya, the data controller or data processor would need to show that the data subject:

- has explicitly consented to the proposed transfer; and
- has been informed of the possible risks of such transfers.

Please note that any sensitive personal data of a data subject requires consent as an additional basis before any transfer out of Kenya.

Following a lawful transfer of personal data, the data controller or data processor is required to make it a condition of the transfer that the personal data is not to be further transferred to another country or territory without the authorisation of the transferring data controller or data processor or another competent authority.

10. Data Protection Officer

A Data Protection Officer may be appointed where:

- The processing is carried out by a public body or private body, except for courts acting in their judicial capacity;
- The core activities of the data controller or processor consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systematic monitoring of data subjects; or
- The core activities of the data controller or the data processor consist of the processing of sensitive categories of personal data.

11. Security

Every data processor or controller must implement appropriate technical and organisational measures to effectively implement the data protection principles and integrate necessary safeguards for data processing.

The Regulations also provide specific obligations in relation to security under the data protection principle of 'Integrity, Confidentiality and Availability'. These obligations have been outlined above in the section on Main obligations and processing requirements.

12. Breach notification

Under the DPA, a data breach is considered as such if:

1. personal data has been accessed or acquired by an unauthorised person; and
2. there is a real risk of harm to the data subject whose personal data has been subjected to unauthorised access.

Under the Regulations, there is a real risk of harm to the data subject if the data breach relates to:

- the data subject's full name or identification number and any of the personal data or classes of personal data relating to the data subject set out in the Regulations; or
- the following personal data relating to a data subject's account with a data controller or data processor—
  - the data subject's account identifier, such as an account name or number; and
  - any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

Once a data breach meets the conditions outlined above, it is considered a notifiable data breach and the data controller is obligated to:

- Notify the Office of the Data Commissioner without delay (within 72 hours) and provide the prescribed information on the data breach: and
- In certain prescribed circumstances, communicate the occurrence of the breach to the data subject in writing.

13. Direct marketing

The DPA does not have specific provisions on direct marketing
A data controller or data processor is considered to be using personal data for commercial purposes if the personal data of a data subject is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction. This definition is expounded on to include circumstances where the personal data is used for direct marketing through:

- sending of a catalogue through any medium addressed to a data subject;
- displaying an advertisement on an online media site where a data subject is logged on using their personal data; or
- sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.

An exception to direct marketing restrictions is provided under the Regulations where the personal data is not used or disclosed to identify or target a particular recipient.

Under the Regulations, personal data other than sensitive personal data may only be used for direct marketing where:

1. the data controller or data processor has collected the personal data directly from the data subject;
2. a data subject is notified that direct marketing is one of the purposes for which personal data is collected;
3. the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;
4. the data controller or data processor provides a simplified opt-out mechanism for the data subject to request not to receive direct marketing communications; or
5. the data subject has not made an opt-out request.

14. Cookies and adtech

Kenyan data protection laws do not make specific provisions for cookies or adtech.

However, depending on the data that is collected through cookies and other adtech, if it includes personal data, it may be considered to be commercial use of personal data or direct marketing.

If data processed through cookies or adtech includes any information relating to an identified or identifiable natural person, the provisions and restrictions on direct marketing and commercial use of personal data will apply. Please see the section above for the provisions on commercial use of personal data and direct marketing.

15. Risk scale

Severe

16. Useful links

The Data Protection Act No. 24 of 2019:
http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019/

The Data Protection (General) Regulations, 2021:
https://www.odpc.go.ke/download/data-protection-regulations/

Cybersecurity

1. Local cybersecurity laws and scope

1. Computer Misuse and Cybercrimes Act, No. 5 of 2018 Laws of Kenya, which provides for cybercrime offences;
2. Kenya Information and Communications Act, No. 2 of 1998 Laws of Kenya which was enacted to facilitate the development of the information and communications sector and electronic commerce;
3. Kenya Information and Communications (Consumer Protection) Regulations, 2010 which was passed to protect consumers of ICT services and products;
4. Data Protection Act, No. 24 of 2019 Laws of Kenya which makes provision for the regulation of personal data, the rights of data subjects and the obligations of data controllers and processors;
5. Guidelines on Cybersecurity for Payment Service Providers, July 2019 which were passed to create a secure cyberspace and combat cybercrime;

2. Anticipated changes to local laws

There are no anticipated changes in the current cybersecurity legislation in Kenya.

3. Application

Computer Misuse and Cybercrimes Act (the "Act")

The Act provides for offences relating to computer systems such an unauthorised access or interference, cyber espionage, cyber harassment, cybersquatting, phishing and cyber terrorism; contains provisions to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; and facilitate international co-operation in dealing with computer and cybercrime matters.

Kenya Information and Communications Act (the "KICA")

The KICA was amended in 2019 to provide for the regulation of electronic transactions and cyber-security by requiring the Communications Authority of Kenya ("CA") to develop a framework for

facilitating the investigation and prosecution of cybercrime offences and promote and facilitate the efficient management of critical internet resources.

Kenya Information and Communications (Consumer Protection) Regulations (the "Regulations")

The Regulations set out the rights and obligations of consumers as well as the safeguards that licensed telecommunication service providers should put in place to protect consumer rights. The Regulations require service providers to take appropriate technical and organisational measures to safeguard the security of its services.

Data Protection Act (the "DPA")

The DPA imposes obligations on data controllers and data processors to provide security measures and mechanisms to ensure the protection of personal data against unlawful destruction, loss, alteration and transfer.

Guidelines on Cybersecurity for Payment Service Providers (the "Guidelines")

Due to the increased cyber threats against banks, the Central Bank of Kenya ("CBK") issued Guidelines to create a safer and more secure cyberspace and establish a coordinated approach to the prevention and combating of cybercrime. The Guidelines set out the minimum standards that Payment Service Providers ("PSPs") should adopt to develop effective cybersecurity governance and risk management frameworks.

4. Authority

Communications Authority of Kenya
https://ca.go.ke/

5. Key obligations

Computer Misuse and Cybercrimes Act (the "Act")

- The Act creates various cybercrime offences by criminalising acts such as unauthorised access or interference, cyber espionage, false publications, child pornography, computer forgery, cyber harassment, cybersquatting, identity theft and impersonation, phishing and cyber terrorism.
- A person who operates a computer system or a computer network, whether public or private, is required to inform the National Computer and Cybercrimes Co-ordination Committee (the "Committee") of any attacks, intrusions and other disruptions to the functioning of another computer system or network within 24 hours of such attack, intrusion or disruption.

Kenya Information and Communications (Consumer Protection) Regulations (the "Regulations")

- The Regulations require service providers to take appropriate technical and organisational measures to safeguard the security of its services.
- Where there is a particular risk of a breach of the security of the network, a service provider is required to inform its subscribers of the risk and of any possible remedies where the risk lies outside the scope of the measures that may be taken by the service provider.

Data Protection Act (the "DPA")

- Where personal data has been accessed or acquired by an unauthorised person and there is a real risk of harm to the data subject, a data controller must notify the Data Commissioner without delay, within 72 hours of becoming aware of the breach.
- The data controller is also required to inform the data subject of the breach unless a restriction is necessary for purposes of prevention, detection or investigation of an offence.

- Offences under the DPA include: disclosure of personal data by data controllers, contrary to the purpose for which the data was collected; disclosure of personal data by data processor without the prior consent of the data controller; obtaining access to personal data without the consent of a data controller or data processor; and offering to sell personal data which has been unlawfully accessed or obtained.

Guidelines on Cybersecurity for Payment Service Providers (the "Guidelines")
The Guidelines impose broad obligations on PSPs requiring them to:

1. Submit a Cybersecurity Policy, Strategies and Frameworks to the Central Bank of Kenya (CBK) by December 31, 2019, for those Operators registered prior to that date and for prospective Operators to submit the same during the licence application process;
2. Notify the CBK within 24 hours of any cybersecurity incidents that could have a significant and adverse impact on the PSP's ability to provide adequate services to its customers, its reputation or financial condition; and
3. Provide CBK with a report concerning its occurrence and handling of cybersecurity incidents on a quarterly basis.

6. Sanctions & non-compliance

Administrative sanctions:

DPA

Under the DPA, the Data Commissioner may serve an enforcement notice on a person who has failed to comply with any provision of the DPA.

The Data Commissioner may also serve a penalty notice to a person who has failed to comply with an enforcement notice requiring the person to pay the amount specified in the notice.

The maximum amount of the penalty is up to KES. 5 million (approx. USD. 50,000) or in the case of an undertaking, up to 1% of its annual turnover of the preceding financial year, whichever is lower.

KICA
Under the Kenya Information and Communications (Consumer Protection) Regulations, the Communications Authority may impose fines of up to KES. 300,000 (approx. USD. 3,000).

Criminal sanctions:

Computer Misuse and Cybercrimes Act

Upon conviction an offender may be liable for a fine ranging between KES. 3 million (approx. USD. 30,000) to KES. 25 million (approx. USD. 250,000) and/or a jail term of between 3 to 25 years.

DPA
The general penalty, for commission of an offence under the DPA is a fine not exceeding KES. 3 million (approx. USD. 30,000), or to an imprisonment term of ten years, or both.

7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?

The National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) was established by the Communications Authority of Kenya as part of its mandate to develop a national cyber security management framework through the establishment of a national computer response team.

The National KE-CIRT/CC's mandate is to coordinate responses, manage cybersecurity incidents

nationally and collaborate with relevant actors locally, regionally and internationally. Its functions include:

1. Implementation of national cybersecurity policies, laws and regulations;
2. Cybersecurity awareness and capacity building;
3. Early warning and technical advisories on cyber threats on a 24/7 basis;
4. Technical co-ordination and response to cyber incidents on a 24/7 basis in collaboration with various actors locally and internationally;
5. Development and implementation of a National Public Key Infrastructure;
6. Research and development in cybersecurity; and
7. Promote and facilitate the efficient management of critical internet resource.

8. National cybersecurity incident management structure

Yes, See above.

9. Other cybersecurity initiatives

The National Cybersecurity Strategy developed by the Ministry of Information Communication and Technology (ICT) defines Kenya's cybersecurity vision, key objectives, and ongoing commitment to support national priorities by encouraging ICT growth and aggressively protecting critical information infrastructures.

The Strategy contains four goals:

1. Enhance the nation's cybersecurity posture in a manner that facilitates the country's growth, safety and prosperity;
2. Build national capability by raising cybersecurity awareness and developing Kenya's workforce to address cybersecurity needs;
3. Foster information sharing and collaboration among relevant stakeholders to facilitate an information sharing environment focused on achieving the Strategy's goals and objectives; and
4. Provide national leadership by defining the national cybersecurity vision, goals and objectives and coordinating cybersecurity initiatives at the national level.

Additionally, the Communications Authority has published the General Information Security Best Practice Guide, which was issued by the CA to be adopted by Kenyan organisations and users across all sectors to enable them to deal with common information security challenges.

The Guide proposes recommendations for common information security challenges such as online safety, unauthorised access, infringement of intellectual property and trade secrets, malware, cloud computing, wireless networks, mobile security, identity theft and fake news.

10. Useful links

The National Kenya Computer Incident Response Team – Coordination Centre:

https://www.ke-cirt.go.ke/

The National Cybersecurity Strategy by the Ministry of ICT:

https://www.ict.go.ke/wp-content/uploads/2016/04/GOKCSMP.pdf

The General Information Security Best Practice Guide by the CA:

https://www.ke-cirt.go.ke/files/2018/05/General-Information-Security-Best-Practice-Guides-for-Kenya-1.pdf

The Second Quarter Cybersecurity Statistics Report for the Financial Year 2019/2020:

https://ca.go.ke/wp-content/uploads/2020/03/Cybersecurity-Sector-Statistics-Report-Q2-2019-2020.pdf

The First Quarter Cybersecurity Statistics Report for the Financial Year 2019/2020:

https://ca.go.ke/wp-content/uploads/2020/02/Cybersecurity-Sector-Statistics-Report-Q1-2019-2020.pdf

Key Contacts

Julius Wako
Nairobi
Partner

Authors

Collette Akwana
Mombasa
Partner

Brian Gatuguti
Nairobi
Senior Associate

Wilson Mrima
Mombasa
Associate