Data Protection Regulations

Ong'anya Ombo Advocates

4th Floor, Windsor House,
University Way, Nairobi, KE.

SUMMARY:

a) **Data Protection (General) Regulations, 2021**

b) **Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021**

c) **Data Protection (Regulation of Data Controllers and Data Processors) Regulations, 2021**

Thinking of initiating legal action/notices (including on matters Data & Privacy, unsolicited or not consented marketing content), please contact us:

m: +254 711 185 636
e: jb@onganyaombo.com

Thinking of enhancing your corporate structures and regulatory compliance (including matters Data & Privacy Law), please contact us:

m: +254 724 026 355
e: om@onganyaombo.com

Data Protection (General) Regulations, 2021

Enabling Rights of a Data Subject

A data controller or processor interested in securing consent must – through written, oral, audio, or video notice – disclose to the data subject its/her/his identity, the purpose of processing, type of personal data, use, possible risks, sharing of data, right to withdraw, and implications of providing, withholding, or withdrawing consent. However, in certain instances, the data processor or controller may bypass all these requirements under a lawful basis as per the meaning of the Data Protection Act (DPA).

The data subject must have the capacity to issue consent for that specific purpose voluntarily. Even where the consent had been given, the data subject may restrict, object to the processing, and request the erasure of the data. Further, the data subject has a right to request access to know the data collected, processed, and stored.

The data subject may apply for rectification of the data. Such applications need to be accompanied by supporting documents.

The Regulations provide for the presumption of consent being freely given unless it is non-negotiable, inability to refuse or withdraw without consequences, merging several actions without seeking consent, or the intention is ambiguous.

In collecting data, the data may be collected indirectly through means such as a third-party, publication/database, surveillance camera, among others – this right is separate from the data subject's data portability rights. After that, a notice must be issued to the data subject.

The data subject has the right to authorise a third party to exercise its rights under the data protection laws.

Restrictions on the Commercial Use of Personal Data

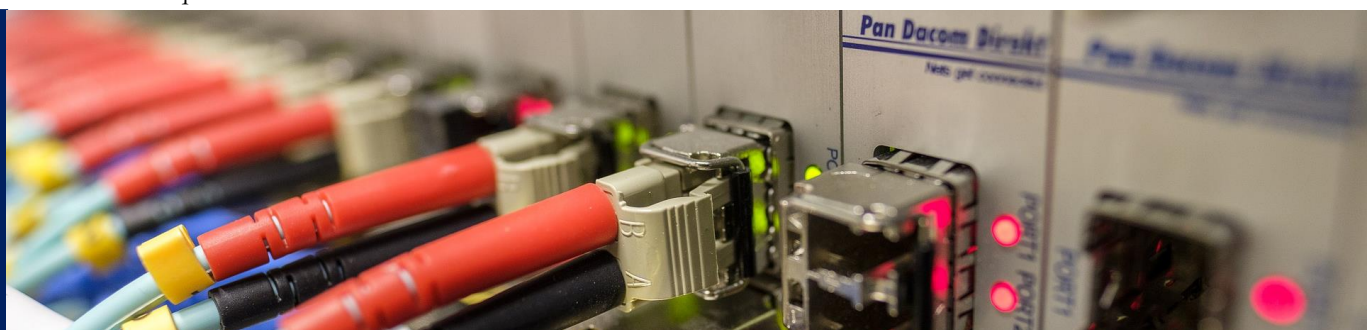
Commercial use entails a series of activities, whether direct or indirect. The data in use ought to be personal data that is not sensitive data as per the DPA. Further, there must be an opt-out option, and no data of the data subject who had opted-out should be used in the commercial activity.

The opt-out mechanism must be practical and be honoured. Further, the data subject may require establishing restrictions on use or disclosures.

Obligations of Data Controllers and Processors

The data controller or processor may legitimately retain the data for a more extended period to meet a particular defined purpose. Thereafter, it may erase, delete, anonymise or pseudonymize the data. The Regulations impose the need to audit the infrastructure holding data.

Factoring in various reasons under the Regulations, the data subject may request that the data processing be done anonymously or pseudonymously. However, the data controller or processor has the discretion to consider the request.



The data controller or processor may share personal data with a third party in reliance on the applicable legal structures.

If the automated individual decision-making measures are incorporated, such will require disclosure and provide more details on the measures, safeguards adopted, relevance, among others, to the data subject.

The data controller can engage a data processor through a contract with standard terms that comply with the law, while the data processor will remain liable to the data controller for the third party it engages.

The processing of personal data for the benefit of the government will require having a data centre and server in Kenya or at least one server copy of the data centre in Kenya.

Elements to Implement Data Protection by Design or by Default

The data protection measures need to comply with the bare minimum of the DPA. The legal principles to factor include lawfulness, transparency, the purpose of limitation, integrity, confidentiality, availability, data minimization, accuracy, storage limitation, and fairness.

Notification of Personal Data Breaches

In the event of a data breach, there is a structure to be adopted when effecting notification concerning that breach. It does not apply to data already in public save where such data is publicly available because of a data breach.

The data controller may request permission from the Commissioner not to communicate the data breach to the data subject.

Transfer of Personal Data Outside Kenya

The data controller or processor needs to confirm compliance with the DPA before transmitting data. Further, there is a need to ensure the entity receiving the data is compliant with data protection measures equally like the DPA.

A country is considered to have the safeguards if it ratified the African Union Convention on Cyber Security and Personal Data Protection, has a reciprocal data protection agreement with Kenya, or contractual binding corporate rules among a concerned group of undertakings or enterprises – and as per the advisory of the Commissioner on places or entities with DPA equivalent protection measures.

In certain instances, the DPA will not affect Kenya's judicial cooperation with other states, and information can be sent to a different location regardless of DPA equivalent compliance if explicit consent is issued and the data subject is informed of the risks involved.

Data Protection Impact Assessment

The Regulations classify certain activities as processing activities that require data protection impact assessment. These activities include large-scale processing of personal data, processing of sensitive data, processing data relating to children, biometric or genetic data, among others.

The Commissioner may carry out periodic audits to monitor compliance.

Exemptions

The Kenya Defense Forces, National Intelligence Services, and National Police Service may be exempted from the provisions of the DPA to the extent that it pertains to National Security. However, the data controller or processor will seek exemption from the Cabinet Secretary. Other exemptions include permitted general situations or permitted health situations.

General Provision

The Data Commissioner projects the discretion of a person aggrieved by a decision of a data controller or processor to lodge a complaint with it.

Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021

The Regulations also adopt a liberal approach to conflict resolution to allow a complainant to lodge a claim without experiencing immense dispute resolution costs and challenges on procedural technicalities.

Procedure for Lodging, Admission, and Response to Complaints

An aggrieved person may lodge a complaint through Form DPC 1 orally, electronic means, or any other means that complies with the DPA's bare minimum. The complaint can be through a representative, in-person, or anonymously. The proceedings will be conducted in Kiswahili, English, or Kenyan Sign Language.

The Data Commissioner will confirm receipt of a complaint within seven days. Thereafter, the complaint will be reviewed for further advice on whether the Data Commissioner has the authority or not – if not, a directive to the best forum will be provided. Also, if the Data Commissioner is of the opinion that there is no legal issue, it will be declined – there is room to be readmitted within six months, where new issues are raised.

The Respondent is required to respond as per the DPA within twenty-one days after receiving that notice.

If an admitted matter does not qualify for further consideration or the complainant refuses, fails, or neglects to communicate without good reasons, the matter will be discontinued – there is room to re-institute a matter.

A party may withdraw a complaint before the determination of the matter. Further, a withdrawn complaint can be re-lodged within six months from the withdrawal date.

If two independent complainants raise an issue or issues that are similar – against one Respondent – the Data Commissioner may request their consent to consolidate the complaint or one to be a test complaint (the outcome of a test complaint automatically gives a determination of a similar complaint). Also, where necessary, the Data Commissioner may order another person to be enjoined to a matter as a party.

ONG'ANYA OMBO ADVOCATES

In conducting its investigation, the Data Commissioner has the authority to summon, administer oath or affirmation, obtain warrants from a court to effect specific actions, among others. Thereafter, in compliance with the Fair Administrative Action Act, the Data Commissioner is required to make a determination that will, among others, address the remedy that the complainant is entitled to.

Remedies include enforcement notice, penalty notice, dismissal, a recommendation for prosecution, or order for compensation to the data subject by the Respondent.

There are other amicable resolution models like negotiation, mediation, or conciliation that the parties can use to reach a desirable outcome.

Enforcement Provisions

The Data Commissioner may issue an enforcement notice detailing the consequence for failing to comply with the penalty notice. The affected party may seek review of the enforcement notice or appeal to the High Court within thirty days from the date of service of the enforcement notice.

The Data Commissioner has the authority to impose a daily fine of not more than ten thousand shillings per day for every single breach as guided by the Public Finance Management Act and enforce or take action to recover upon the lapse of defined statutory timelines.

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

The Regulations apply to all data controllers or processors that do not fall under the realm of Data Protection (Civil Registration) Regulations, 2020.

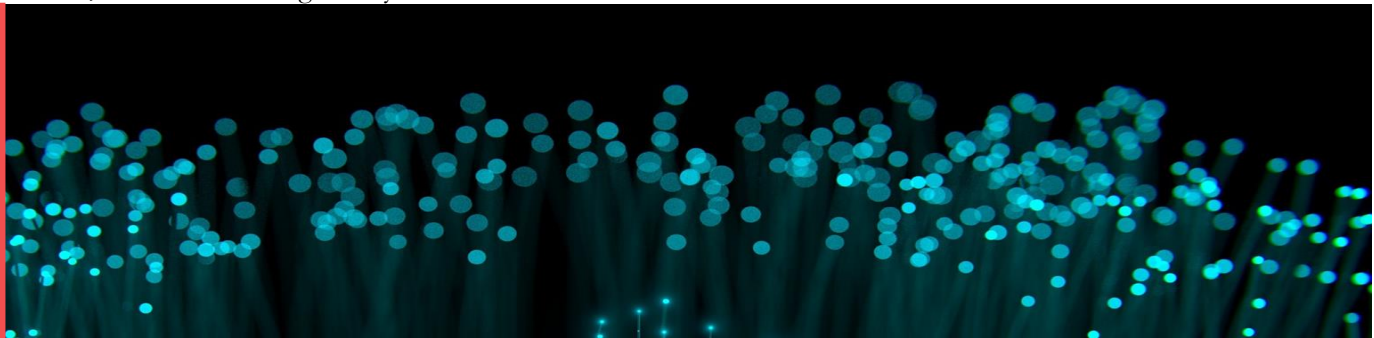
A data controller determines the purpose and means for processing personal data while a data processor processes personal data on behalf of the data controller, excluding employees of the data controller. The data processor must also have a contractual relationship with the data controller and no authority on the purpose and means of processing personal data. However, if the data processor processes the data beyond its instructions, it will also be regarded as a data controller.

A person who is both a data controller and processor will apply for both statuses. The registration process will be conducted electronically via the Data Commissioner's website.

Registration fees will accompany the application for registration. The application will include documents identifying the person, a description of the purpose for which personal data is processed, and a description of the personal data being processed.

The payment of fees by State or County department will pay fees for their entities that operate within that department, must be funded by the Consolidated Fund, and provides public service. The regulation is also applied towards State or County Corporations.

If the Data Commissioner is satisfied with the contents of the application while considering the regulatory factors, a certificate lasting twenty-four months will be issued – the certificates are renewable.



In the event of refusal, the applicant may reapply in compliance with the recommendations provided in the refusal notice.

A renewal notice may require further verification if the renewal covers new areas that were initially not covered under the initial certificate.

There are exemptions from mandatory registration that apply to a data controller or processor with an annual turnover or annual revenue below five million shillings, has less than ten employees. The exemption does not waive the need to be registered, comply with Principles and Obligations of Personal Data Protection and Transfer of Personal Data Outside Kenya as per the DPA.

A data controller or processor with an annual turnover below five million shillings processing personal data per the third schedule will not be covered under the exemptions.

There will be a register detailing registered data controllers or processors that will be updated every thirty days. The registered persons will experience variation or cancellation based on requests by the person or audits conducted by the Data Commissioner.

Processing personal data without complying with the DPA, provision of false or misleading information to secure registration, or fails to renew but continue to process personal data will result in an offence with penalties as provided under the DPA.