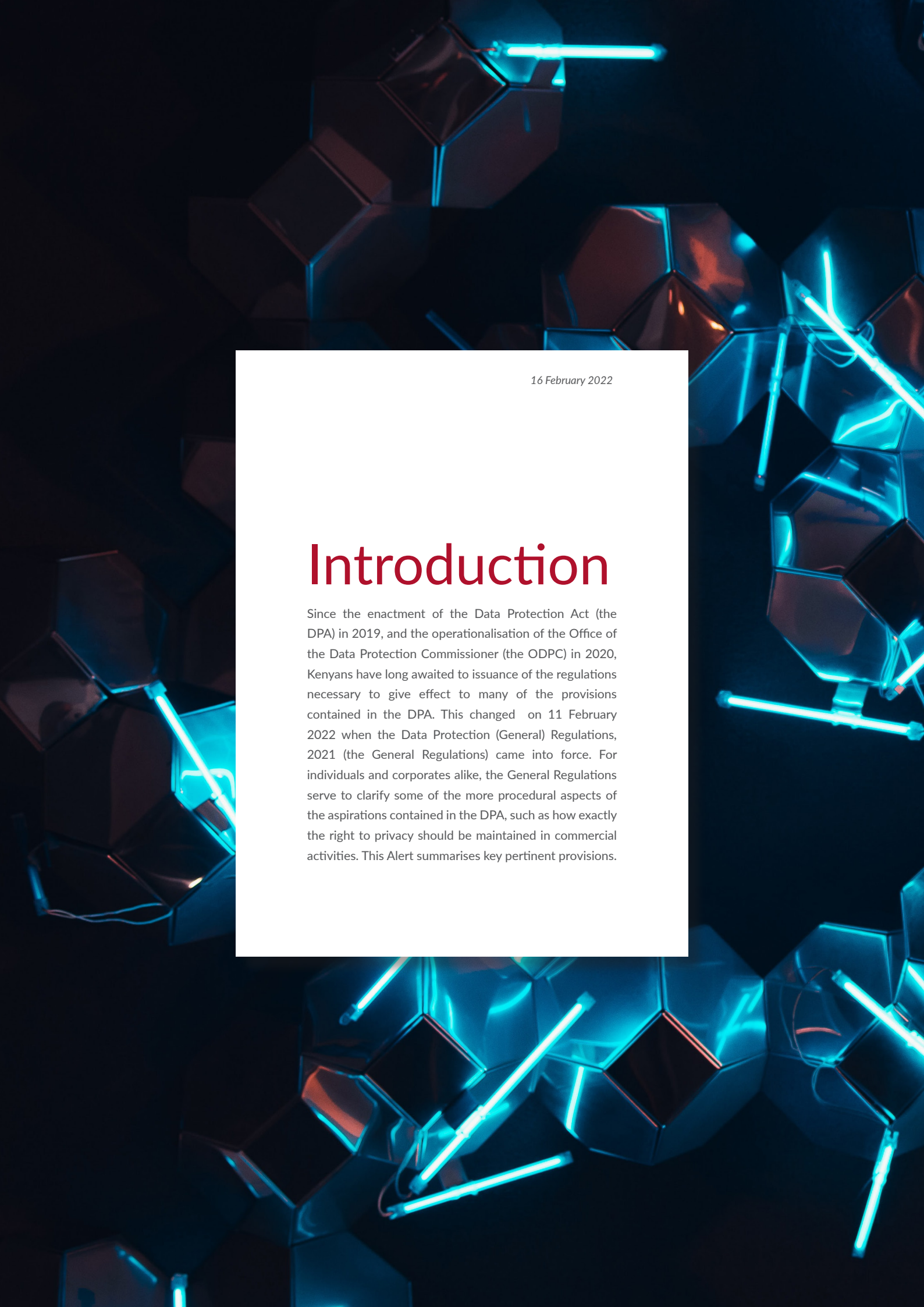
Data Protection (General) Regulations, 2021

LEGAL ALERT

ALGERIA
CÔTE D'IVOIRE
GUINEA
KENYA
MADAGASCAR
MALAWI
MAURITIUS
MOROCCO
NIGERIA
RWANDA
SUDAN
TANZANIA
UGANDA
ZAMBIA
• • •
UAE



16 February 2022

Introduction

Since the enactment of the Data Protection Act (the DPA) in 2019, and the operationalisation of the Office of the Data Protection Commissioner (the ODPC) in 2020, Kenyans have long awaited to issuance of the regulations necessary to give effect to many of the provisions contained in the DPA. This changed on 11 February 2022 when the Data Protection (General) Regulations, 2021 (the General Regulations) came into force. For individuals and corporates alike, the General Regulations serve to clarify some of the more procedural aspects of the aspirations contained in the DPA, such as how exactly the right to privacy should be maintained in commercial activities. This Alert summarises key pertinent provisions.

Enabling the Rights of a Data Subject

The General Regulations prescribe various instances that trigger obligations on data controllers and data processors to fulfil the rights of a data subject.

a) Consent as a pre-requisite to data processing

Consent can be relied on as a lawful basis for processing of personal data under the DPA. In seeking consent, the data controller/data processor is required to inform the data subject of the following:

i. the identity of the data controller or data processor;

ii. the purpose of each of the processing operations for which consent is sought;

iii. the type of personal data that is collected and used;

iv. the possible risks arising from cross-border data transfers due to absence of an adequacy decision or appropriate safeguards in the recipient jurisdictions;

v. whether the personal data processed will be shared with third parties; and

vi. the data subject's right to withdraw consent.

A data controller or data processor must ensure that the data subject has capacity to give consent, gives it voluntarily and the consent is specific to processing before obtaining consent. Emphasis is placed on freely given consent. Consent cannot be obtained as part of non-negotiable terms of a contract, or be based on the threat of detrimental consequences in the event a data subject opts to withhold it. For example, requiring online shoppers to consent to receive promotional emails in order to complete an online purchase would be invalid consent due to the preconditions imposed on completing the transaction.

b) Lawful basis for processing

Data processing can only rely on one legal basis at a time, which has to be established before the processing. For example, if a data controller or data processor is relying on consent as a lawful basis of processing, they cannot also rely on the basis of performance of a contract at the same time. Additionally, where a data controller uses multiple bases for different processing, the data controller must distinguish between the legal bases being used and respond to any request from a data subject about the legal bases. Therefore, it is important for a data controller or a data processor to analyse which basis for processing they wish to rely on before initiating the process of obtaining consent from a data subject.

c) Mode of collection of personal data and restriction to processing

Personal data must be collected directly from the data subject unless specific exceptions apply. Personal data may be collected indirectly in various instances such as where the data subject has consented to the indirect collection or where the data subject has deliberately made the personal data publicly available.

In processing indirectly collected data on the basis of a data subject's consent, a data controller or data processor must ensure that processing is limited to personal data which the data subject has consented to. For every instance of indirectly collected personal data, the data controller or processor must undertake steps to ensure that personal data is accurate, limited to only that which is necessary for the purpose, and up to date. They should also secure personal data and to comply with the lawful processing principles. For example, if a data subject permits a third-party application to collect personal information from a social media account, the third-party application must ensure that it only collects and processes the scope of personal data permitted by the data subject (e.g., username and email), and in doing so, must ensure it complies with the data protection principles laid out in the DPA.

Data subjects also have the power to restrict the processing of their personal data on various grounds. Data subjects can restrict processing where data subjects contest the accuracy of their personal data or where the data subjects oppose the erasure of personal data in the event of unlawful processing and requests restriction instead. Processing may also be restricted where the data subjects no longer need their personal data but the data controller or data processor requires the personal data to be kept in order to establish, exercise or defend a legal claim.

A data controller or data processor may decline to comply with a request for restriction in processing, where such request is manifestly unfounded or excessive. The General Regulations do not specify what types of requests would be considered 'manifestly unfounded or excessive'. According to the United Kingdom's Information Commissioner's Office (ICO) a manifestly unfounded request is one where the individual clearly has no intention of exercising their right or makes a request which is malicious in intent. Excessive requests are those which are, on the face of it, unreasonable. The ICO advises that determining if a request is manifestly unfounded or excessive is highly contextual. A key indicator used is if the request is repetitive in nature. For example, if a data subject systematically sends different requests as part of a clear campaign to cause disruption, this could be deemed to be manifestly unfounded. Another example of this could arise if a data subject makes a request which repeats the substance of a previous one, or overlaps with another request.

d) Data access request

Data subjects have a right to obtain from the data controller or data processor confirmation as to whether or not personal data concerning them is being processed. In such a scenario, they can request access to the personal data and information on the purposes for which the processing is taking place and details on the categories of personal data concerned. Therefore, it is imperative that a data controller or data processor maintain records that clearly document information relating to personal data that may be required to be furnished for a data access request.

e) Rectification of Personal data

Where personal data is untrue, inaccurate, outdated, incomplete or misleading a data subject may request a data controller or data processor to rectify the data.

f) Rights of erasure – the right to be forgotten?

Data subjects may request a data controller or data processor to erase or destroy personal data which they hold where:

i. the personal data is no longer necessary for the purpose for which it was collected;

ii. the data subjects withdraw their consent that was the lawful basis for retaining the personal data;

iii. the data subjects object to the processing of their data and there is no overriding legitimate interest to continue the processing;

iv. the processing of personal data is for direct marketing purposes and the individual objects to that processing;

v. the processing of personal data is unlawful; or

vi. the erasure is necessary to comply with a legal obligation.

A right of erasure is not absolute. For example, a request for erasure may be declined if the personal data needs to be retained in compliance with a legal obligation or for the performance of a task in the public interest.

Restrictions on the Commercial Use of Personal Data

A data controller or processor is considered to use personal data for commercial purposes where commercial or economic interests are sought after, primarily through direct marketing. Examples of direct marketing include sending catalogues to data subjects through any medium, displaying advertisements on online media sites where data subjects are logged on using their personal data or sending electronic messages to data subjects about sales or other advertising material. A data controller or processor is allowed to use personal data, other than sensitive personal data, concerning a data subject for the purpose of direct marketing where:

i. the data controller or data processor has collected the personal data from the data subject;

ii. a data subject is notified that direct marketing is one of the purposes for which personal data is collected;

iii. the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;

iv. 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

v. the data subject has not made an opt out request.

Using personal data for commercial purposes without the consent of the data subject is an offence and on conviction, one is liable to a fine of up to KES 20,000 or to a term of imprisonment of up to 6 months, or to both. These penalties are comparatively less than those recently imposed by data protection authorities in jurisdictions such as the United Kingdom and the European Union. For example, We Buy Any Car, an online car purchasing service, was fined GBP 200,000 by the

ICO for sending 191 million marketing messages and 3.6 million SMS messages in contravention of the UK's Privacy and Electronic Communications Regulations.

Obligations of Data Controllers and Data Processors

a) Retention of personal data

Personal data processed for a lawful purpose may only be retained for as long as may be reasonably necessary for the purpose for which the personal data is processed. Data controllers or data processors are required to establish a personal data retention schedule which provides for the periodic review of the personal data held to establish whether it is no longer necessary or whether the prescribed retention period has lapsed. Where either of these is the case, the data controller or data processor must erase, delete, anonymise or pseudonymise such personal data.

b) Requests to Deal Anonymously or Pseudonymously

Data subjects may request a data controller or data processor to process their personal data anonymously or pseudonymously in the following instances:

i. where they do not wish to be identified;

ii. to avoid subsequent contact such as direct marketing from an entity or third parties;

iii. to enhance their privacy on their whereabouts;

iv. to access services such as counselling or health services without it becoming known to others;

v. to express views in a public arena without being personally identified; or

vi. to minimise the risk of identity fraud.

c) Sharing of Personal Data

A data controller or data processor may share or exchange personal data collected, upon request, by another data controller, data processor, third party or a data subject. In such an instance, the data controller or data processor is required to determine the purpose and means of sharing personal data from one data controller or data processor to another. However, the sharing of personal data must be undertaken subject to the principles of personal data protection in the DPA. This is distinct from international data transfers, which are subject to further restrictions.

d) Automated Individual Decision Making

Where automated individual decision making is undertaken, the data controller or data processor is required to:

a. inform a data subject when engaging in processing based on automated individual decision making;

b. provide meaningful information about the logic involved;

c. ensure:

   i. specific transparency and fairness requirements are in place;

   ii. rights for a data subject to oppose profiling and specifically profiling for marketing are present; and

   iii. where required, a data protection impact assessment is carried out;

d. explain the significance and envisaged consequences of the processing;

e. ensure the prevention of errors;

f. use appropriate mathematical or statistical procedures;

g. put appropriate technical and organisational measures in place to correct inaccuracies and minimise the risk of errors;

h. process personal data in a way that eliminates discriminatory effects and bias; and

i. ensure that a data subject can obtain human intervention and express their point of view.

e) Data Protection Policy

Data controllers or data processors must develop, publish, and regularly update a policy reflecting their handling practices for personal data. Such policies may include various provisions including the nature of personal data collected and held, how a data subject may access their personal data and exercise their rights in respect to that personal data, complaints handling mechanisms, lawful purpose for processing personal data and obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya.

f) Contract Between Data Controller and Data Processor

Data controllers must have written contracts in place for their engagements with data processors. The General Regulations set out basic provisions which must be in these contracts, such as the provision of adequate safeguards by the data processor.

g) Obligations of a Data Processor

A data processor must not engage the services of a third party for processing data without the prior authorisation of the data controller and once authorisation is given, the data processor must enter into a contract with the third party, including the same basic provisions as those in the contract between the data controller and the data processor.

h) Requirement for a Specified Processing Data to be Done in Kenya

A data controller or data processor who processes personal data for strategic interests of the state is required to process such personal data through a server and data centre located in Kenya or store at least one server copy of the concerned personal data in a data centre located in Kenya.

Strategic interest includes the processing of personal data for the purpose of administering of the civil registration and legal identity management systems (e.g., the Huduma Number), facilitating the conduct of elections, overseeing any system for administering public finances by any state organ (e.g. the Integrated Financial Management Information System), running any system designated as a protected computer system, offering any form of early childhood education and basic education under the Basic Education Act, 2013 or provision of primary or secondary health care for a data subject in the country.

Notification of Personal Data Breaches

Certain categories of data breaches should be notified to the Data Commissioner. They include where a data breach relates to:

i. 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 as provided in the General Regulations; or

ii. the data subject's account identifier with the data controller or processor, 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.

Breach notifications should include, among other things, the date and circumstances of the breach and a chronological account of the steps taken by the data controller or data processor following the breach.

Transfer of Personal Data Outside Kenya

In order to transfer personal data out of Kenya, a data controller or data processor must satisfy several conditions which we set out below.

a) appropriate data protection safeguards

A transfer outside Kenya would be based on appropriate safeguards where there is a legal instrument containing appropriate safeguards for the protection of personal data that is essentially equivalent to the protection under the DPA and the General Regulations. Appropriate safeguards would also apply if the data controller, having assessed all the circumstances surrounding transfers of a particular type of personal data concludes that appropriate safeguards exist to protect the data.

Appropriate safeguards are also deemed to be in place where the recipient country has ratified the African Union Convention on Cyber Security and Personal Data Protection or has a reciprocal data protection agreement with Kenya or where there are contractually binding corporate rules among a concerned group of undertakings or enterprises. The concept of contractually binding corporate rules is borrowed from the EU and entails related entities (e.g., a group of companies) operating across several countries developing data protection policies which govern the cross border transfer of personal data. As adopted in the EU, such policies must include all data protection principles and provide for the enforcement of data subjects' rights. They must also be binding on all members of the group.

b) an adequacy decision made by the Data Commissioner

The Data Commissioner may publish on its website a list of countries, and territories for which an adequate level of protection is ensured.

c) transfer as a necessity

Personal data may be transferred on the basis of necessity in the following instances:

i. for the performance of a contract between the data subject and the data controller or data processor;

ii. for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

iii. for any matter of public interest; or

iv. for the establishment, exercise or defence of a legal claim.

c) consent of the data subject

In the absence of an adequacy decision, appropriate safeguards or prerequisites are required for transfer as a necessity. A transfer of personal data to another country shall take place only on the condition that the data subject has explicitly consented to the proposed transfer and has been informed of the possible risks of such transfers.

Data Protection Impact Assessment (DPIA)

Under the DPA, a DPIA ought to be conducted where a processing operation is likely to result in high risk to the rights and freedoms of a data subject. We will discuss this in further detail in our alert on the Guidance Note on DPIAs issued by the OPDC which will be published as part of this series.

Exemptions under the DPA

The General Regulations provide for various exemptions in relation to the data protection regime as described below:

a) Exemption for national security

Where data is processed by either the Kenya Defence Forces, National Intelligence Service or the National Police Service, such processing is exempt from the requirements under the DPA and the General Regulations. However, a data controller or processor who processes personal data for the national security organs and wishes to be exempt on that ground needs to apply to the Cabinet Secretary for an exemption.

b) Exemption for public interest

Exemptions relating to public interest occur in two scenarios:

i. Permitted general situation

A data controller or processor may collect, use, or disclose personal data for, amongst other reasons, lessening or preventing a serious threat to the life, health, or safety of any data subject, or to public health or safety; taking appropriate action in relation to suspected unlawful activity or serious misconduct; or locating a person reported as missing.

ii. Permitted health situation

A data controller or data processor may collect, use or disclose personal data in situations involving the collection of health information to provide a health service; the collection, use, or disclosure of health data for health research and related purposes; or the use or disclosure of genetic information obtained in course of providing a health service based on necessity of use or disclosure in such circumstances.

Conclusion

The publication of the General Regulations is a welcome move as it will guide data controllers and data processors in instituting the necessary internal mechanisms to comply with the DPA as well as provide greater clarity on provisions of the DPA that required detailed rules for their implementation.

If you need any advice in relation to the General Regulations, please do not hesitate to reach out to our Data Protection Team (dataprotectionteam@africalegalnetwork.com)

Key contacts

Should you require more information, please do not hesitate to contact:

Sonal Sejpal

Partner
ALN Kenya | Anjarwalla & Khanna

ss@africalegalnetwork.com

Anne Kiunuhe

Partner
ALN Kenya | Anjarwalla & Khanna

ak@africalegalnetwork.com

Wangui Kaniaru

Partner
ALN Kenya | Anjarwalla & Khanna

wk@africalegalnetwork.com

Contributors

Charlotte Patrick-Patel (Senior Associate)

Jade Makory (Associate)

Abdulmalik Sugow (Trainee Lawyer)

Abdullahi Ali (Trainee Lawyer)

The content of this alert is intended to be of general use only and should not be relied upon without seeking specific legal advice on any matter.