TECHNOLOGY, MEDIA & TELECOMMUNICATIONS
ALERT

31 JANUARY 2022

CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

IN THIS ISSUE

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

In part one of this three-part series, Cliffe Dekker Hofmeyr (CDH) Kenya will unpack the salient features and provisions of the Data Protection (General) Regulations of 2021 (the General Regulations).

FOR MORE INSIGHT INTO OUR EXPERTISE AND SERVICES

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

In part one of this three-part series, Cliffe Dekker Hofmeyr (CDH) Kenya will unpack the salient features and provisions of the Data Protection (General) Regulations of 2021 (the General Regulations).

CONSENT

The Data Protection Act (DPA) provides that the data subject's consent may be relied upon as a ground for lawfully processing personal data. It provides that consent must be a statement or clear affirmative action that is unequivocal, free, specific, informed and that signifies agreement to the processing of personal data.

The General Regulations go further to stipulate the following requirements and obligations which data controllers or processors must discharge in relation to consent to the processing of personal data. These are broken down into three key components; notification requirements where consent is relied upon as the ground for processing personal data, capacity to grant consent, and opt-in requirement for consent.

1. **Notification requirements where consent is relied upon as the ground for processing personal data**

Regulation 4(1) of the General Regulations requires data controllers or processors to notify data subjects of several matters while seeking their consent prior to processing their personal data. These include a notice of:

- the purpose of each of the processing operations for which consent is sought;
- the type of personal data that is collected and used, information about the use of the personal data for automated decision-making, where relevant etc.
- the identity of the data controller or data processor etc.

A subsequent number of the notifiable matters in this context are not expressly required to be notified to data subjects under Section 29 of the DPA, which sets out the notification requirements to be observed by data controllers or processors at the point of collection of personal data. It is, however, arguable the notifiable matters set out in the regulations should still be notified to data subjects by virtue of the application of the principle requiring data controllers or processors to ensure that personal data is processed lawfully, fairly and in a transparent manner.

Therefore it is important for businesses that process personal data, either as data controllers or processors, and that rely on data subject consent as a basis for such processing activities, to update their privacy notices to include all the matters that are required to be notified to data subjects under the General Regulations in this context. In addition, Regulation 4(3) of the General Regulations also leaves room for oral, as well as audio and video recorded communication, of the notifiable matters to the data subject in addition to or as an alternative to the written privacy notices.

2. **Capacity to grant consent**

Regulation 4(3) of the General Regulations requires data controllers or processors to ensure that the data subject has capacity to give consent, that they give it voluntarily and that the consent is specific to the purpose of the processing.

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

The voluntary nature of consent, is additionally under the DPA's requirement for consent to be "*free*" and the obligation to ensure that it is specific to the purpose of the processing is also covered under the DPA. The obligation to ensure that the data subject has capacity to provide consent is however broader under the General Regulations than it is under the DPA. The DPA's capacity verification requirements are restricted to age verification mechanisms and a requirement for consent to be obtained from a data subject's parents/guardians where the data subject is a child. The General Regulations do not set out any definition of the term "*capacity*". The DPA and the Data Commissioner's Guidance Note on Consent also offer no definition of this term and as such capacity could be construed as extending beyond capacity as determined on the basis on age. Hence, data controllers must now also put in place mechanisms for verifying other matters that could go towards verification of capacity to give consent such as soundness of mind, illness etc. This is certainly a point on which further guidance from the Data Commissioner would certainly be useful (especially in respect of measure that the Data Commissioner recommends on how data controllers and data subjects ought to go about verifying the additional elements of capacity without risking violating a data subject's right to privacy.

3. Opt-in requirement for consent

Regulation 4 (a) of the general Regulations also indicates that consent will not be deemed to have been freely given if it is based on a data subject's failure to object to the processing of their data. This regulation underscores the requirement for consent to be expressly given by the data subject (i.e., the data subject should expressly opt-in or agree to the processing of their personal data either by words to that effect or by way of a clear affirmative action. Any processing of personal data on the basis of consent that is inferred from the data subject's failure to opt-out of or disagree to the processing of their personal data would therefore be unlawful.

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

DEVELOPMENTS ON THE OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

The General Regulations expound on various obligations of Data Controllers and Data Processors are provided for under the DPA to a significant degree. the new requirements that gave been stipulated under the General Regulations will give effect to the obligations of data controllers and data processors as provided for under the DPA.

1. **Obligations in relation to the retention of personal data**

Data controllers or data processors are required to:

- establish personal data retention schedules with appropriate time limits for the periodic review of the need for the continued storage of personal data that is no longer necessary or where the retention period is reached; and
- erase, delete anonymise or pseudonymise personal data upon the lapse of the purpose for which the personal data was collected.

2. **Obligations in relation to automated individual decision making**

The General Regulations define automated individual decision making as a decision made by automated means without any human involvement and introduce a raft of obligations which must be fulfilled by a data controller or processor when automated individual decision making in the processing of personal data. These include:

- informing the data subject when engaging in processing based on automated individual decision making;
- providing meaningful information about the logic involved;
- processing personal data in a way that eliminates discriminatory effects and bias;
- ensuring that a data subject can obtain human intervention and express their point of view etc.

3. **Obligation in relation to privacy policies**

The DPA does not set out an express requirement for a privacy policy. It does, however, set out notification requirements that are to be met at the point of collection of personal data. These notification requirements were typically met by most data controllers and data processors through having written privacy policies.

The General Regulations have now however set out a mandatory requirement for data controllers and data processors to develop, publish and regularly update a policy reflecting their personal data handling practices.

TIMELINES IN RELATION TO OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS UNDER THE DPA

The General Regulations have introduced several new timelines for compliance with obligations under the DPA or under its own provisions. These are unpacked as; indirect collection of personal data, requests for Restriction of processing of personal data, data access requests, requests for rectification of personal data, requests for data portability, and requests for erasure.

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

1. Indirect collection of personal data

According to Section 28 of the DPA requires data controllers or data processors to collect personal data directly from the data subject save for in specified situations where it allows for the collection of personal data indirectly from other sources. The General Regulations go further to introduce a new requirement for data controllers or data processors who collect personal data indirectly to inform the data subject of such collection within 14 days.

Businesses that rely on the indirect collection of personal data (such as schools hotels, restaurants/catering establishments, insurance companies and tax revenue agencies) under the grounds permitting such collection under the DPA should make a careful note of this new timeline.

2. Requests for Restriction of processing of personal data

In Section 34 of the DPA data controllers or data processors to restrict the processing of personal data at the request of a data subject under certain specified circumstances. Whilst, Section 34(3) of the DPA also required data controllers or data processors to implement mechanisms to ensure that time limits set for restriction of processing of personal data are observed.

In this regard, Regulation 7(3) of the General Regulations also introduce a new requirement for data controllers or data processors to implement, free of charge, when any request from a data subject for the restriction of the processing of their personal data within 14 days of the date of such a request. In addition, within this 14-day window, it must be indicated on their systems that the processing of any such personal data has been restricted and give notice of the restriction to third parties with whom the relevant personal data may have been shared.

3. Data Access Requests

Section 25(b) of the DPA provides data subjects with a right to access their personal data which is in the custody of a data controller or data processor. The General Regulations go further to state that this right entitles the data subject to seek confirmation from the data controller or data processor as to whether personal data about them is being processed. Where it is being processed, the data subject has the right to access such personal data and certain stipulated information such as the purpose for the processing, the categories of personal data concerned etc. The General Regulations also require data controllers or data processors to provide a data subject with access to their personal data on request and requires them to provide the data subject with a copy of such personal data. Data controllers or data processors are interestingly also now specifically required to put in place mechanisms to enable a data subject to proactively access or examine their personal data.

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

Data controllers or data processors are now also required to comply with a data subject request for access to their personal data within 7 days of any such request.

4. Requests for Rectification of Personal Data

The DPA and the General Regulations provide data subjects with a right to request the rectification of any of their personal data, which is untrue, inaccurate, outdated, incomplete or misleading. Where the data controller or data processor is satisfied that a rectification is necessary, they will be required to rectify the relevant entry of personal data in the database within 14 days of the request for rectification.

5. Requests for Data Portability

The DPA and the General Regulations provide data subjects with a general right to request and receive their personal data in a structured, commonly used and machine-readable format from a data controller or data processor and to transmit the same to another data controller or data processor (data portability). The DPA and the General Regulations require data controllers or data processors to port personal data to the data subject's choice of recipient within thirty days of the request and upon payment of the prescribed fees. The DPA and the General Regulations make provision for the decline of such a request but in that event the General Regulations require a data controller or data processor to notify the data subject of the decline and the reasons for such decline in writing 7 days.

6. Requests for Erasure

The DPA and the General Regulations provide data subjects with a general right to request, free of charge, for the erasure or destruction of their personal data that is within the data controller's or data processor's custody and stipulate the situations where such requests may be made which include where the personal data is no longer necessary for the purpose for which it was collected or is excessive or was obtained unlawfully or is processed unlawfully etc. Data controllers and data processors now are required under the General Regulations to respond to a request for erasure of their personal data within 14 days.

COMMERCIAL USE OF PERSONAL DATA AND DIRECT MARKETING

General Rule

The DPA provides that personal data should not be used for commercial purposes save where the data subject has consented to such use, or the data controller or data processor is authorised by law to make such use of the personal data. Regulation 14 of the General Regulations expressly provide that a data controller or data processor is deemed to use personal data for commercial purposes where they use it to advance commercial or economic interests.

The General Regulations also highlight that a data controller or data processor is considered to use personal data to advance commercial interests where personal data is used for direct marketing through certain specified ways including

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

sending an electronic message to a data subject about a sale using personal data provided by a data subject. The General regulations also clarify that marketing is not direct marketing where personal data is not used or disclosed to identify or target recipients.

1. Permitted use of personal data for direct marketing

The circumstances in which personal data may be used for direct marketing have been clarified under the General Regulations (15) as follows as being the following:

- where the personal data has been collected directly from the data subject;
- where the data subject is notified that the personal data is collected for direct marketing purposes;
- the data subject has consented to the use or disclosure of the personal data for that purpose;
- 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
- the data subject has not made an opt out request

The use of the conjunction *"or"* as opposed to *"and"* suggests that direct marketing may be carried out when any one of the above circumstances exist independently. However, that understanding would contradict the opt-in mechanics that are envisaged under consent as a ground for processing personal data, the principle of privacy as provided for under section 25 of the DPA and indeed the spirit of the data protection law. In our view this provision ought to be amended to replace *"or"* with *"and"* to require all five circumstances above to subsist at the same time before direct marketing can be undertaken. We therefore recommend, out of an abundance of caution, that enterprises that run direct marketing campaigns using personal data ought to ensure that the all the above-listed circumstances subsist before they proceed to run such campaigns.

2. Restrictions on use of personal data for direct marketing

The General Regulations also prohibit the sending of direct marketing messages without details of the address to which requests for a cessation of such messaging may be sent free of charge. The General Regulations also prohibit the use of direct marketing messaging where:

- the identity of the person on whose behalf the communication has been sent has been disguised or concealed;
- a valid address to which the recipient of the message may send a request for cessation of the messaging has not been provided; or
- there is use of automated calling systems without human intervention.

The General Regulations 13(2)(b) It should also be noted that any direct marketing related profiling of a data subject who is a child is prohibited.

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

Further, according to Regulation 17(1), General Regulations and 17(4) direct marketing messaging must now include a prominently displayed statement drawing the data subject's attention to the fact that the data subject may make an opt out request and must also provide a data subject with an option to opt out of all future direct marketing communications.

The upshot of this is that the use of personal data for direct marketing messaging is subject to the data subject's absolute right to object to the same, according to Regulation 8(4) and (5), of General Regulations. However, Regulation 12(1)(d) state, the use of personal data for direct marketing is also subject to a general right of the data subject to request for the erasure or destruction of their personal data.

This is further underscored by the fact that the General Regulations go further to set out that an offence is committed where a data controller or data processor uses personal data for commercial purposes without the consent of the data subject. The offence is punishable, upon conviction, by a fine not exceeding twenty thousand shillings or to a term of imprisonment not exceeding six months, or to both fine and imprisonment.

DATA PROTECTION BY DESIGN OR BY DEFAULT

According to Section 41of the DPA requires every data controller or data processor to implement appropriate technical and organisational measures which are designed to implement the data protection principles in an effective manner and to integrate necessary safeguards for that purpose into the processing. The General Regulations sets out eight separate provisions that delineate the elements that are necessary to implement six of the eight principles of data protection as provided for under section 25 of the DPA.

The setting out of these practical elements in detail is particularly useful in decrypting the actual manner of implementing data protection by design or by default in the operations of data controllers and data processors. For example, some of the elements that have been stipulated for purposes of implementing the integrity and confidentiality principle are:

- using audit trails and event monitoring as a routine security control;
- having in place routines and procedures to detect, handle, report, and learn from data breaches;
- regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing etc.

Implementing data protection by design or by default mechanisms is an intensely practical exercise. It is advisable for data controllers and data processors to work closely with ICT and legal experts to ensure that their personal data management systems as are demonstrably aligned with the requirements set out under the General Regulations as possible as the level of compliance with the prescribed data protection by

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

design or by default elements will be pertinent in determining culpability of the data controllers or data processors in the event of any data breaches that occur.

NOTIFICATION OF PERSONAL DATA BREACHES

Section 43(1) of the DPA provides that where personal data has been accessed or acquired by an unauthorised person, and there is a real risk of harm to the relevant data subject, a data controller shall notify the data commissioner within 72 hours and without delay and also communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established and subject to any need for non-disclosure so as to facilitate the prevention, detection or investigation of an offence by the concerned relevant body.

The General Regulations have set out a critical elucidation of this notification obligation in providing that a data breach is taken to result in real risk of harm to a data subject if that data breach relates to:

- the data subject's full name or identification number and any of the personal data or classes of personal data set out in the Second Schedule to the General Regulations including the data subjects' salary, credit card number etc.; 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 data subject's account.

The General Regulations provide that a breach of any personal data that is deemed to result in real risk of harm to a data subject as per the above criteria would be notifiable under section 43 of the Act. The General Regulations also stipulate the details of the contents of the breach notification that is required to be sent to the Data Commissioner where a breach occurs. These include:

- details on how the notifiable data breach occurred, where applicable;
- the number of data subjects or other persons affected by the notifiable data breach;
- the personal data or classes of personal data affected by the notifiable data breach;
- the potential harm to the affected data subjects due to the notifiable data breach etc.

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

TRANSFER OF PERSONAL DATA OUTSIDE KENYA

The General Regulations have introduced general principles of cross-border personal data transfer. The principles require a data controller or data processor who is a transferring entity to ascertain that the transfer is based on following before the transfer of personal data out of Kenya is carried out:

- appropriate data protection safeguards;
- an adequacy decision made by the Data Commissioner;
- necessity; or
- consent of the data subject.

The General Regulations then go further to define the circumstances that would constitute ach of the above principles and thereby justify a transfer of personal data out of Kenya. Of great interest is the introduction of the principle of adequacy decisions which is borrowed from the European Union where data protection regulators are empowered to issue such decisions regarding jurisdictions that are deemed to have proper data protection laws and safeguards and to which personal data from the European Union may be safely transferred subject to other requirements. The issuance of a such decisions would to a great degree ease the transfer of personal data to the jurisdictions marked as having adequacy safeguards, a factor that would ease the administrative and economic burden of having to secure an alternative ground for such transfers and facilitate business operations that are dependent on such movement of personal data. It will therefore be interesting to see if the Data Commissioner will move quickly to publish a list of jurisdictions that the ODPC deems to have adequate data protection safeguards for purposes of cross border transfers out of Kenya.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Section 31 of the DPA requires data controllers or data processors to carry out a DPIA prior to starting any processing operations where such operations (by virtue of their nature, scope, context and purposes) are likely to result in high risk to the rights and freedoms of data subjects.

The General Regulations have set out a further elucidation of this obligation in providing a list of the processing operations that are to be considered to result in high risks to the rights and freedoms of data subjects including:

- use of personal data on a large-scale for a purpose other than that for which the data was initially collected;
- processing biometric or genetic data;
- large scale processing of personal data;
- a systematic monitoring of a publicly accessible area on a large scale.

KENYA

Part 1: Unpacking the Data Protection (General) Regulations, 2021 of the Data Protection Act 24 of 2019

CONTINUED

As such, data controllers or data processors that carry out any of the processing operations that result in high risks to the rights and freedoms of data subjects including those operations set out in the list that is provided under the General Regulations must conduct a DPIA prior to processing personal data.

Section 31(3) of the DPA requires data controllers and processors to consult the Data Commissioner if a DPIA that has been conducted indicates that he contemplated processing of personal data would result in high risks to the rights and freedoms of data subjects. The General Regulations have gone further to stipulate that such consultations must be done within 60 days from the date of receipt of the DPIA report by the data controller or data processor.

SHEM OTANGA AND
RICHARD ODONGO

OUR TEAM

For more information about our Technology, Media & Telecommunications practice and services in South Africa and Kenya, please contact:

Christoff Pienaar
Practice Head
Director
T +27 (0)21 481 6350
E christoff.pienaar@cdhlegal.com

Preeta Bhagattjee
Director
T +27 (0)11 562 1038
E preeta.bhagattjee@cdhlegal.com

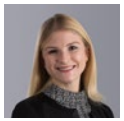
Shem Otanga
Partner | Kenya
T +254 731 086 649
+254 204 409 918
+254 710 560 114
E shem.otanga@cdhlegal.com

Njeri Wagacha
Partner | Kenya
T +254 731 086 649
+254 204 409 918
+254 710 560 114
E njeri.wagacha@cdhlegal.com

Aphindile Govuza
Senior Associate
T +27 (0)11 562 1090
E aphindile.govuza@cdhlegal.com

Richard Odongo
Associate | Kenya
T +254 731 086 649
+254 204 409 918
+254 710 560 114
E richard.odongo@cdhlegal.com

Lee Shacksnovis
Associate
T +27 (0)21 481 6453
E lee.shacksnovis@cdhlegal.com



Mieke Vlok
Associate
T +27 (0)21 481 6442
E mieke.vlok@cdhlegal.com

BBBEE STATUS: LEVEL ONE CONTRIBUTOR
Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

PLEASE NOTE
This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196.
Private Bag X40, Benmore, 2010, South Africa.
Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111
E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001.
PO Box 695, Cape Town, 8000, South Africa.
Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388
E ctn@cdhlegal.com

NAIROBI
Merchant Square, 3rd floor, Block D,
Riverside Drive, Nairobi, Kenya.
P.O. Box 22602-00505, Nairobi, Kenya.
T +254 731 086 649 | +254 204 409 918 |
+254 710 560 114
E cdhkenya@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central,
Stellenbosch, 7600.
T +27 (0)21 481 6400
E cdhstellenbosch@cdhlegal.com

CDH
CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA