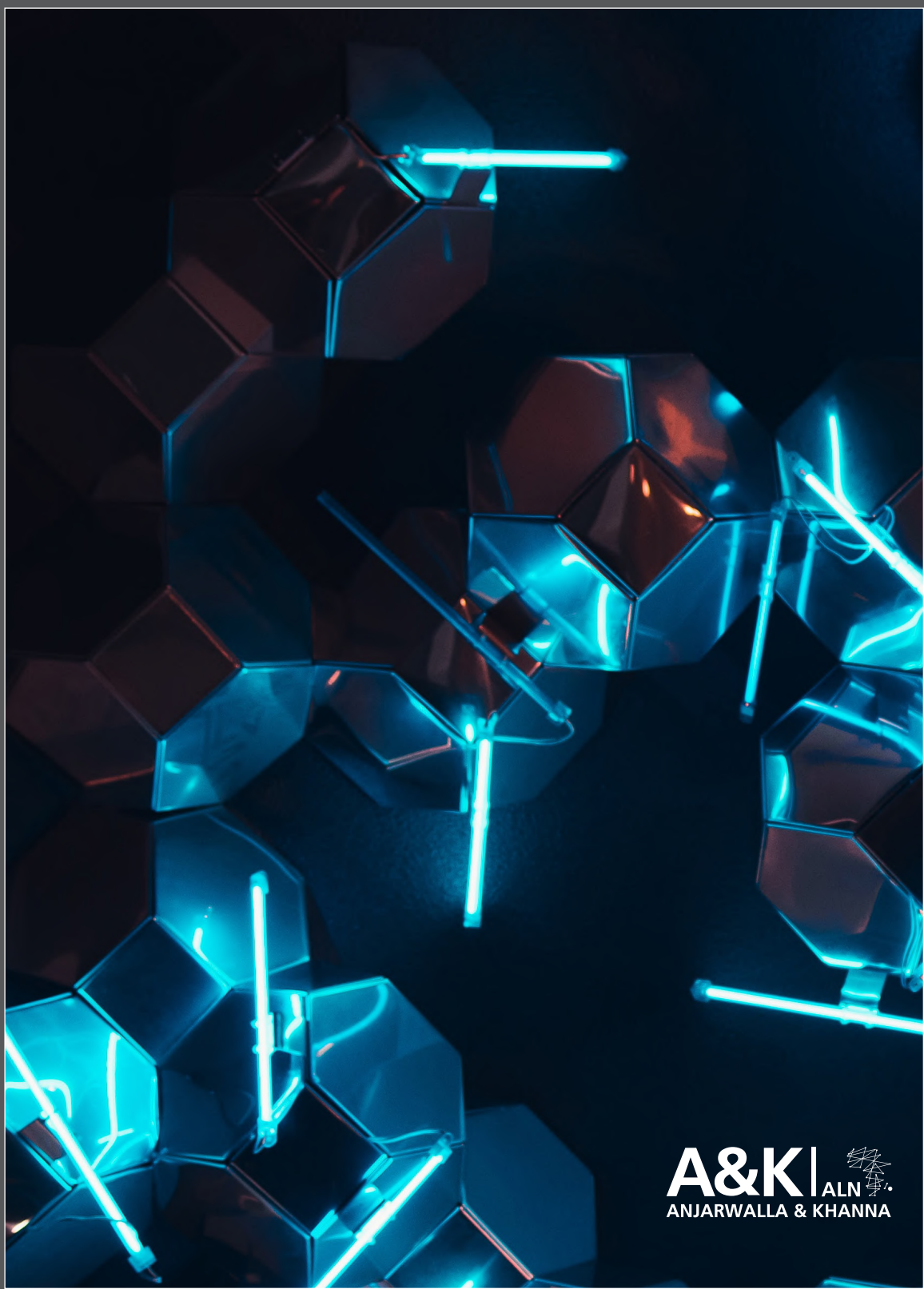
Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021

LEGAL ALERT

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



18 February 2022

Introduction

From July 2022, your organisation may have to register with the Office of the Data Protection Commissioner (ODPC). Approximately two years after the enactment of the Data Protection Act (the DPA), the Cabinet Secretary for Information Communication and Technology, Innovation and Youth Affairs has issued the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 (the Registration Regulations).

The Registration Regulations will give much needed guidance on the requirements you have to meet to register as either a data processor or a data controller. We briefly set out the key things you should know.

Data Controller or Data Processor?

Data controllers determine the purpose and means for processing personal data while data processors process personal data on behalf of data controllers. Usually, data processors have a contractual relationship with data controllers and do not exercise any decision-making power on the purpose and means of processing personal data. While the employees of a data controller may process data on behalf of their employer, they are excluded from being deemed to be data processors.

If a data processor exceeds the scope of instructions from the data controller, they would be deemed to be data controllers for purposes of assessing liability in respect of that specific activity. If you act as both a data controller and data processor, you are required to apply to be registered in both capacities, and to pay the requisite fees for each.

For illustrative purposes, in an employment context, an employer who uses a business processing service provider to run payroll would be deemed to be a data controller, while the payroll service provider would be a data processor. Even though the employer's staff may carry out some processing in connection with running the payroll, such staff would not be deemed to be data processors. If the service provider acts beyond the scope of instructions, it would be held liable as though it were the data controller in relation to that specific processing activity.

Exemptions

All civil registration entities (such as the Office of the Registrar of Persons which issues national identity cards) specified in the earlier issued Data Protection (Civil Registration) Regulations, 2020 are exempt from the Registration Regulations. Aside from this exemption, the Registration Regulations also exclude the following data controllers and data processors from mandatory registration:

i. those with an annual turnover of below KES 5 million or an annual revenue of below KES 5 million; **and**

ii. with less than 10 employees.

The turnover threshold is applicable to non-profit making data controllers and data processors such as charitable and religious institutions, and 'turnover' is defined as the utilised budget of such entities in the year preceding their application for registration.

Despite being exempt, these entities are still required to comply with provisions of Parts IV and V of the DPA which relate to the Principles and Obligations of Personal Data and Grounds for Processing of Sensitive Personal Data.

Entities processing personal data for the following activities, listed in the Third Schedule of the Registration Regulations, are not exempt from mandatory registration even if their revenue or turnover is below KES 5 million and they have less than 10 employees:

i. canvassing political support among the electorate;

ii. crime prevention and prosecution of offenders (including operating security CCTV systems);

iii. gambling;

iv. operating an educational institution;

v. health administration and provision of patient care;

vi. hospitality industry firms but excludes tour guides;

vii. property management including the selling of land;

viii. provision of financial services;

ix. telecommunications networks or service providers;

x. businesses that are wholly or mainly in direct marketing;

xi. transport services firms (including online passenger hailing applications); and

xii. businesses that process genetic data.

Given that the aim of the exemptions appears to be to minimise compliance costs for smaller organisations, it may have been more practical to exempt them from paying a registration fee rather than from the requirement to register with the ODPC. This is because such organisations are still required to comply with the DPA irrespective of their registration status and the cost of such compliance would be similar to non-exempt entities. A notable example of this approach was adopted in the United Kingdom (UK) by the Information Commissioner's Office, where certain organisations do not have to pay a fee to register as data controllers. Non-registration may have the undesirable effect of removing data controllers and data processors from the purview of the ODPC which may put the rights of data subjects at risk.

This position seems to have been adopted as, based on our reading, the Registration Regulations require mandatory registration of exempt entities. Earlier drafts of the Registration Regulations also provided the same thresholds for exemption while indicating that entities involved in the activities listed in the Third Schedule would not qualify for exemption. However, the final version which is currently in force includes a provision to the effect that entities which meet the exemption thresholds would still be required to undergo mandatory registration. It therefore remains to be seen how the ODPC will give effect to the exemptions in practice considering the conflicting positions in the Registration Regulations.

Application Procedure, Registration, and Renewal

The Registration Regulations prescribe a form for making an application for registration as a data controller and data processor. Applicants will need to disclose, among other things, the purpose for which they process personal data and a description of the categories of personal data they intend to process. All applications must be accompanied by an applicant's constitutional documents which will vary depending on the legal structure. The Registration Regulations provide that the ODPC should administer the application process electronically

through its website. The ODPC's website indicates that the application portal will be coming up soon.

Once an application is submitted, and the ODPC is satisfied that the applicant has met the requirements, a certificate is granted within 14 days and the registration is valid for a renewable period of 24 months. However, in the event the applicant seeks to expand the scope of its registration during renewal, for example by including further categories of personal data or purposes of processing, the ODPC will treat the renewal as a new application. If an applicant is unsuccessful in either the initial or renewal application, the ODPC is required to communicate its refusal to grant registration or renewal within 21 days, accompanied with the reasons for refusal. An application may be rejected for reasons such as providing insufficient particulars, a lack of appropriate safeguards for personal data and violations of the DPA. Upon rejection, applicants may apply afresh after having rectified the specified reasons for refusal.

The ODPC is required to maintain a register of all data controllers and data processors on its website. If a data controller or data processor changes its particulars, it must notify the ODPC in writing.

The ODPC reserves the right to cancel or vary the conditions of a certificate of if:

i. a data controller/data processor applies for variation or cancellation;

ii. the ODPC establishes that the information provided in registration was false or misleading; or

iii. the data controller/data processor wilfully or negligently fails to comply with provisions of the DPA and any regulations made under it.

Category	Registration fees (KES) (payable once)	Renewal fees (KES) (payable every 2 years)
Micro and Small Data Controllers/ Data Processors 1-50 employees; and < KES 5 million revenue/turnover	4,000	2,000
Medium Data Controllers/Data Processors 51-99 employees; and 5,000,001-50 million revenue/ turnover	16,000	9,000
Large Data Controllers/Data Processors > 99 employees; and > KES 50 million revenue/turnover	40,000	25,000
Public entities	4,000	2,000
Charities and religious entities	4,000	2,000

Registration-Related Offences

The following offences attract a penalty under section 73 of the DPA:

i. a failure to update the ODPC of a change in particulars;

ii. processing personal data without registering;

iii. providing false or misleading information for the purpose of registration; and

iv. failing to renew a certificate of registration and continuing to process personal data after the expiry of the certificate.

The maximum penalty prescribed under section 73 of the DPA is a fine of up to KES 3,000,000 and a term of imprisonment of up to 10 years, or both.

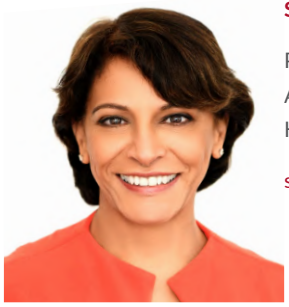
Conclusion

With the Registration Regulations in force, it is incumbent on all data processors and data controllers to register with the ODPC to avoid attracting penalties under the DPA to avoid significant penalties for non-compliance.

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)

Olivia Njoroge (Trainee Lawyer)