KICTANet
The Power of Communities

Memorandum

Technical Brief on the ODPC registration process and independence of data protection authorities

Date: 18th September 2023

The National Assembly Ad-Hoc Committee on the inquiry into activities and operations of Worldcoin in Kenya

Honourable Chair and Members,

The Kenya ICT Action Network (KICTANet) is a multi-stakeholder think tank for ICT policy and regulation. As a stakeholder in the technology policy sector, we would like to submit to the Committee our views on the following points with the aim of guiding the Committee on what we believe would be good for the country after the recent discourse surrounding Worldcoin and the regulation of emerging technology in general.

KICTANet seeks through this submission to give technical guidance on the application of data protection regulations as is provided in the Data Protection Act of 2019 as well as to provide a technical briefing on the interplay between data protection regulation and emerging technology. We hope that this will shed more light to the matter at hand, as well as guide in the development of further knowledge as the country continues to build its capacity for technology regulation.

In this memorandum, we address two things, namely:

- ☐ Registration of Data Controller and Processors and the legal differentiation with complaince.
- ☐ The independence of the data protection authorities.

Registration of Data Controllers and Processors

The Data Protection Act of 2019 in PART III requires data controllers and data processors to be registered. The provisions under this part state that organisations processing personal information must register as data protection controllers or processors and pay registration fees unless they qualify for an exemption. Entities are required to renew their data protection registration every

two years unless registration is no longer required based on the criteria set in the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

"18. (1) Subject to sub-section (2), no person shall act as a data controller or data processor unless registered with the Data Commissioner.
(2) The Data Commissioner shall prescribe thresholds required for mandatory registration of data controllers and data processors, and in making such determination, the Data Commissioner shall consider —

(a) the nature of industry;
(b) the volumes of data processed;
(c) whether sensitive personal data is being processed; and
(d) any other criteria the Data Commissioner may specify.

19. (1) A data controller or data processor required to register under section 18 shall apply to the Data Commissioner.
(2) An application under sub-section (1) shall provide the following particulars —

(a) a description of the personal data to be processed by the data controller or data processor;
(b) a description of the purpose for which the personal data is to be processed;
(c) the category of data subjects, to which the personal data relates;
(d) contact details of the data controller or data processor;
(e) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data;
(f) any measures to indemnify the data subject from unlawful use of data by the data processor or data controller; and
(g) any other details as may be prescribed by the Data Commissioner.

(3) A data controller or data processor who knowingly supplies any false or misleading detail under sub-section (1) commits an offence.
(4) The Data Commissioner shall issue a certificate of registration where a data controller or data processor meets the requirements for registration.
(5) A data controller or data processor shall notify the Data Commissioner of a change in any particular outlined under subsection (2).
(6) On receipt of a notification under sub-section (5), the Data Commissioner shall amend the respective entry in the Register.
(7) A data controller or data processor who fails to comply with the provisions of this section commits an offence.

20. A registration certificate issued under section 19 shall be valid for a period determined at the time of the application after taking into account the need for the certificate, and the holder may apply for a renewal of the certificate after the expiry of the certificate."

The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 was drafted to enable the ODPC to implement the Data Protection Act requirement of registration in a society that has been grappling with understanding the concept of data protection compliance. Therefore, the requirements upon registration did not require one to have complied with the Act during registration, rather Registration was/is the first step towards compliance with the Act.

Why is registration required and is it complete data protection compliance?
The answer to this is Yes, still only partially, it is required and it is in compliance with Section 18 of the Act. The other answer is that registration only is not complete compliance. There is much more that is required to be compliant with the Act. Registration happens to be one important element of compliance with the data protection legislation as entities, including individuals, cannot act as Data Controllers or Data Processors in Kenya unless they have registered with the ODPC.

It is important to note that Registration is not a requirement unique to Kenya. All East African nation-states with data protection laws require registration. The United Kingdom of Great Britain and Japan also require data controllers and processors to be registered.

World over, registration with a data protection authority is generally just one aspect of compliance with data protection laws. Compliance encompasses a wide range of activities, including developing data processing records, developing a privacy framework and implementing it, developing privacy policies, controls and notices, and conducting data protection impact assessments, the list is endless. Data protection compliance is not an event, it is a journey with good days and bad days.

Data protection registration requirements and conducting due diligence

The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 provide in detail what is required for the registration as a data controller and data processor. The requirements for registration include:

- a copy of establishment documents;
- particulars of the data controllers or processors including name and contact details;
- a description of the purpose for which personal data is processed E.g. for payroll, invoicing, Know Your Customer (KYC), registration, etc.
- a description of categories of personal data processed e.g. name, address, Identification number;
- a description of categories of data subjects e.g. employee, client, students, supplier, shareholder
- recipient (s) to whom personal data is (are) disclosed e.g. KRA, CBK among other requirements as per the regulations.
- The previous annual turnover/revenue of the entity seeking to be registered.
- Put measures in place for the protection of personal data by identifying risks to personal data (E.g. unauthorized access/disclosure, theft, etc.) and putting Safeguards, security measures and mechanisms implemented to protect personal data (E.g. Access control, visitors' logbook, privacy policy, information security policy, etc.)
- For data controllers and data processors to familiarize themselves with the provisions of the Act and adopt practices that promote compliance.

A review of the above-listed requirements clearly shows that ODPC's mandate in registration does not extend enhanced due diligence in order for an entity to be registered. The registration process is of an administrative nature and it should be this way for the sake of ease of doing business. Many countries across the world require registration to only have administrative checks but they do not have complete due diligence processes to ensure an organisation is fully compliant before registering them.

Case Studies: Japan

Japan

In Japan, the supervisory authority, PPC reviews registration documents for compliance, and this process is primarily focused on administrative and procedural aspects. The PPC does not conduct in-depth due diligence or assessments of data controllers' overall data protection practices, data security measures, or compliance with all aspects of APPI as part of the registration process.

Instead, the PPC relies on data controllers to self-assess their compliance with APPI and fulfill their legal obligations. If there are concerns or issues related to data protection or privacy compliance, they may be addressed through audits, investigations, or enforcement actions by the PPC or other relevant authorities.

The United Kingdom

The Information Commissioner's Office (ICO) in the United Kingdom does not typically conduct due diligence in the form of comprehensive audits or assessments of data controllers' data protection practices before accepting registration. The registration process with the ICO is primarily administrative in nature, and data controllers are generally responsible for ensuring their own compliance with data protection laws, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

While the ICO does not conduct due diligence as part of the registration process, it has the authority to conduct audits and investigations if it suspects non-compliance with data protection laws. If issues are identified, the ICO may take enforcement actions, including fines or other corrective measures.

Full compliance with the Data Protection Act is not required before one is registered. However, one has to show that they are working on complying with the Act.

As the world digitises by the minute and new technologies are being put to use, it is important that individuals know how entities that are processing their data comply with the law, which helps increase trust and contributes to economic growth. Registration also gives the ODPC an additional tool to promote Data Protection compliance and effectively regulate the processing of data to minimize potential harm, damage or distress caused to individuals.

In the case in point as soon as investigations were undertaken on the activities of Worldcoin the regulator issued an enforcement notice and suspended their activities for 12 months. This ensured fair administrative action that is required in order to ensure predictability in regulation that heavily contributes to the ease of doing business as well as investor confidence in the regulatory frameworks governing data in Kenya. Registration and enhanced due diligence that is undertaken during compliance must not be conflated.

The independence of the data protection authorities

Key points about independence

The independence of the DPA is a cornerstone of data protection, and an independent supervisory body is the key element of all international data protection agreements and standards.

The matter of independence has been addressed by the United Nations in the Paris Principles –a set of international standards adopted by the General Assembly in 1993, which define the role, composition, status, and functions of National Human Rights Institutions.

Independence of the DPAs is guaranteed by EU primary law since the adoption of the Lisbon Treaty and GDPR, which in article 52 explicitly states that "each supervisory authority shall act with complete independence in performing its tasks and exercising its powers" and that members of the authority shall "remain free from external influence, whether direct or indirect and shall neither seek nor take instructions from anybody." There is an important case law from the Court of Justice of the European Union (CJEU) underlining the need to ensure the independence of DPAs[1] due to their fundamental role in monitoring the application and ensuring compliance with data protection law, as well as acting as guardians of the rights of citizens as far as their privacy and personal data are concerned. E.g., in a case brought by the European Commission, the Court ruled that the abrupt termination of the Hungarian Data Protection Commissioner's term in office by the government constitutes an infringement of the independence of the Hungarian Data Protection Authority and is hence in breach of EU law.

Convention 108 (the only legally binding international treaty in the data protection field) and its modernised version - Convention 108+ considers independence as an essential component of the data protection supervisory system in a democratic society. According to Article 15.5 of the Convention, the supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.

Global Privacy Accesmbly (GPA), which ODPC joined in 2022, set specific criteria for its members, including "appropriate autonomy and independence". A Background Document on the Interpretation of the Autonomy and Independence Criteria[2] states that independence is important for agencies to be able to operate free from political or governmental interference and to withstand the influence of vested interests.

An example of privacy revelations followed by parliamentary inquiries and investigation by DPA

While DPAs cannot be aware of and prevent all possible violations, timely and effective reactions to revelations through press reports, complaints or other sources of information and the

combination of preventive and dissuasive measures and robust enforcement actions make a data protection system successful.

Here is an example of a recent privacy revelation followed by parliamentary inquiries and DPA actions:

Cambridge Analytica

In 2017-2018, tech giant Facebook and data analytics firm Cambridge Analytica were at the centre of a dispute over the harvesting and use of personal data. US senators have called on Mark Zuckerberg to testify before Congress about how Facebook will protect users, while in the UK, the chairman of a Culture, Media and Sport of Parliamentary Committee, has summoned Mr Zuckerberg to explain the "catastrophic failure" to MPs.

The UK parliamentary inquiry looked into both Facebook's own use of personal data to further its business interests and examined what Facebook claimed as 'abuse' of its platform by the disgraced political data company Cambridge Analytica — which in 2014 paid a developer with access to Facebook's developer platform to extract information on millions of Facebook users in build voter profiles to try to influence elections.[3]

During the inquiry, the parliamentary committee closely worked with the data protection supervisory authority - the Information Commissioner's Office (ICO) and as lawmakers wondered whether the authority had the resources, power and political backing to take on a privacy investigation involving one of the world's biggest tech companies.[4] ICO submitted the report to the parliamentary committee [5], based on which, along with the other evidences, the parliamentary committee issued the final report [6] and supported the recommendations from the ICO.

Conclusion

There are other privacy scandals where DPAs have acted on company's misuse of data after receiving complaints such as the case of Clearview AI, where the Data Protection Authorities in the EU and UK have acted against the company's mishandling of data after receiving complaints and public debate on the risk paused by its activities was growing. (see for e.g., the decision from the French DPA).

More generally speaking, data protection authorities have limited resources that they have to allocate to different and equally important – missions (privacy education, guidance, enforcement, and answering citizens' queries and complaints). Therefore, data protection authorities are not expected and do not have the legal authority and resources, in Kenya or any other modern privacy system around the world, to continuously investigate/police the entire domestic "data space". This is why it is important to invest in developing a culture of compliance and strengthening DPAs are essential.

References

1. Case C-518/07 European Commission v Federal Republic of Germany [2010] ECLI:EU:C:2010:125; Case C-614/10 European Commission v Republic of Austria [2012] ECLI:EU:C:2012:631; Case C-288/12 Commission v Hungary [2014] ECLI:EU:C:2014:237; Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.
2. https://globalprivacyassembly.org/wp-content/uploads/2019/12/ICDPPC-Background-document-on-independence-criteria_post-Coe-comment.pdf
3. https://techcrunch.com/2019/02/17/uk-parliament-calls-for-antitrust-data-abuse-probe-of-facebook/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACdC5ULhFdB6vy4m0q5rY633IAKX1WGdqbVzpO-Hu5Lyh_eXsmnJc7YUKTAceXLA7NeOO49XhmJvQHG6PQXt9s7PSs5woVyTFTRAzWhModFiO09ERHPTCdjk-UrKD0dvVC4G05mefRo7fjgtWArqz36SZmBk_qXdGL76Empog71q
4. https://www.politico.eu/article/cambridge-analytica-scandal-thrusts-uk-data-protection-chief-into-eye-of-storm/
5. Investigation into the use of data analytics in political campaigns (ico.org.uk)
6. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf