

Data Protection Alert

Celebrating International Data Privacy Day

January 2024

To ensure compliance data controllers and processors have to carry out gap assessments to identify privacy loopholes within their organisations and develop implementation roadmaps to remedy identified gaps

A glance at the strides made by the Rwanda Data Protection Law

Rwanda enacted its Law relating to Protection of Personal and Privacy Law N° 058/2021 of 13/10/2021 (the “DPP”) in October 2021 and provided a two year transition period for individuals and organisations operating as data controllers and/or data processors to comply with this Law.

The DPP governs the processing of personal data which is defined as information relating to an identified or identifiable natural person (“data subject”). It imposes notable obligations on organisations which are established or resident in Rwanda or organisations which are situated outside Rwanda but process personal data of data subjects in Rwanda.

The DPP also introduces the concept of a designated representative which requires data controllers and data processors who are neither established or reside in Rwanda but process personal data of data subjects in Rwanda, to designate a representative to comply with organisation’s obligations under this Law.

Similar to most data protection and privacy laws, the DPP is largely informed by the European Union’s General Data Protection Regulations (“GDPR”) which was enacted on 25 May 2018. Most of the principles that are included in the DPP mirror the GDPR and this is the standard across multiple countries over the world, as the GDPR is considered the bedrock of all data protection laws.

However, there are some elements of the DPP which are unique to the Rwanda jurisdiction and cannot be traced down to the GDPR. For instance, the data subject right to representation of minors and medically impaired data subjects, and the



right to designate an heir are also such examples.

As we celebrate the international data privacy day, we reflect on some of the biggest trends in data privacy in Rwanda from the past two years and look ahead at what we anticipate will come, we also look at the progress that the Rwanda Law has made so far.

More recently, the National Cyber Security Authority (NCSA) was entrusted with the responsibility to supervise the enforcement and implementation of the DPP. In March 2022 the NCSA launched the Rwanda Data Protection Office (DPO) to be the regulator on its behalf.

A year later the DPO developed a portal within their [website](#) where data controllers and processors can access standard registration application forms and instructions of how to submit the forms to the DPO via email. The DPO also has a complaint lodging section where aggrieved persons may access the [complaint forms](#) and the instructions for submission. This gives people a platform to report any data protection related issues to the regulator. The registration portal is yet to be activated, meanwhile all the applications for registration are being done manually.

There have also been a lot of initiatives from the DPO aimed at sensitising key stakeholders including data controllers, data processors, and the data subjects, on the legal framework of the data protection law and the obligations of these stakeholders under this law. The DPO has introduced guidelines ([here](#)) for registration of data controllers and data processors on the DPO website.

These guidelines outline the step by step process ([here](#)) for registering with the DPO as a data controller or a data processor. The guidelines also give guidance on the designation of a data protection officer ([here](#)),

personal data inventory readiness assessment [here](#), and data protection impact assessment guide and form ([here](#)).

Another key highlight of the DPP which the DPO has effectively operationalised is the requirement for authorisation to transfer personal data outside of Rwanda. The DPO has now put in place mechanisms to ensure that applicants can access the application forms and a breakdown of the requirements for authorisation. An example of one such requirement is that a data controller or processor seeking authorisation to transfer personal data outside of Rwanda must have carried out a DPIA of high risk processing activities. This is in alignment with international best practice.

There has also been progress in the application for registration process where the DPO has set up an online application portal where data controllers and data processors can access the application forms. The website of the DPO also has a portal for facilitating the lodging of complaints, and also has a number of guidelines including guidelines for registration, for data inventories, and for lodging complaints. This has been a big win for the NCSA because it

has ensured standard practice and uniformity in the implementation of the DPP.

Moreso, following the operationalisation of the DPP in October 2023 the regulator expects that all data controllers and processors have registered with the DPO, appointed a data protection officer, developed a record of processing activities, carried out a data protection impact assessment (DPIA), and conducted training and awareness on data protection. These are just some examples of the key compliance requirements under the DPP.

Additionally, to ensure compliance data controllers and processors have to carry out gap assessments to identify privacy loopholes within their organisations and develop implementation roadmaps to remedy identified gaps within their organisations.

Failure to demonstrate compliance may attract administrative penalties and fines from the regulator. PwC has managed to support various clients across different sectors in their journey towards compliance. Data controllers and data processors are now exposed to hefty fines of up to one percent (1%) of the global turnover for the preceding financial year in the event of a data breach.

Globally, the most recent developments relate to the European Union's Artificial Intelligence Act (AI Act) which was provisionally agreed on by EU's three key institutions; the European Commission, Council and Parliament in early December 2023.

This law provides for a comprehensive legal framework for artificial intelligence development and deployment within the EU and beyond. This regulation sets out certain systems which will be prohibited including biometric categorisation systems that model data based on characteristics such as political, religious, race, philosophical beliefs etc, high risk AI systems and foundational models and general purpose AI.

Organisations will be required to use technical information provided by AI to conduct data protection





impact assessment. The final text of the regulation was published early this week for initial thoughts and deliberations by EU member states before final voting. Some of the emerging privacy issues will relate to establishing internal privacy governance structures and controls for AI systems and advising clients on how to comply with the AI regulation.

Even though Rwanda has not yet developed any framework for the regulation of AI, the ministry of ICT through the Centre for the Fourth Industrial Revolution Rwanda (C4IR Rwanda) is currently working on drafting AI policy and ethical guidelines including supporting the

government of Rwanda in developing its national AI policy.

Notwithstanding the impressive strides that the DPP has taken in Rwanda so far, a number of challenges are inevitable. The current challenges include interpretation of the law, which is relatively new and yet to be interpreted by any law courts in Rwanda.

The supervisory authority is yet to publish any comprehensive procedural guidelines on how businesses operating in Rwanda can comply with the DPP. This potentially creates some grey areas where compliance becomes hindered.

In conclusion, as we mark data privacy day 2024, organisations operating in Rwanda should take stock of the new regulatory environment that they operate in, which is marked by a new and active privacy regulator.

Organisations that fail to take action now expose themselves to potential regulatory sanctions as well as loss of customer trust and brand reputation.

It is therefore imperative that you choose the right advisers that can demonstrate the relevant mix of expertise, experience and competencies to support you on your privacy compliance journey.

For further information on the Rwanda Data Protection and Privacy Law, please contact any of the people below or your usual PwC contact.



Joseph Githaiga
Director and head of Legal
Business Solutions
joseph.githaiga@pwc.com
PwC Kenya



Frobisher Mugambwa
Head of Tax &
Fiscal Policy Leader
frobisher.mugambwa@pwc.com
PwC Rwanda



Tracy Odipo
Senior Associate
Legal Business Solutions
tracy.odipo@pwc.com
PwC Rwanda



Kesly Kayiteshonga
Senior Associate
Legal Business Solutions
kesly.kayiteshonga@pwc.com
PwC Rwanda



Blissful Dzimiri
Associate
Legal Business Solutions
blissful.dzimiri@pwc.com
PwC Rwanda



Kelvin Rwamushaija
Associate
Legal Business Solutions
kelvin.rwamushaija@pwc.com
PwC Rwanda