Data Protection Alert

Second of the series: Registration of a Data Controller and a Data Processor

This second alert forms part of a three-part series on Rwanda's Personal Data Protection and Privacy Law. The first alert covered the "General Overview of the Rwanda Data Protection and Privacy Law" while the next alert will cover storage and transfer of personal data according to the Law relating to the Protection of Personal Data and Privacy (Nº 058/2021 of 13/10/2021).

February 2023

The data protection Law has no registration thresholds, therefore any entity that collects or processes personal data in Rwanda will be required to register with the NCSA by 15 October 2023

The importance of protecting data is rapidly increasing due to advances in technology, legislation, and client/individual demands. Increasingly, many firms and companies in Rwanda handle a significant amount of data, some of it being client data or employee data, and some of it is personal data and sensitive personal data. Both the data controller and the data processor have the responsibility to limit, protect and respect personal data.

The Rwanda Data Protection and Privacy Law (the "Law") aims at achieving a robust level of data protection and the appropriate use of personal data, thus the need to register both the data processor and the data controller with the National Cyber Security Authority (NCSA) through its Data Protection Office (the "DPO"). The Law takes effect on 15 October 2023. From this date, data controllers and processors will be expected to comply with the requirements of the Law.

Key terms

Data controller: natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines the means of their processing.

Data processor: natural person, public or private corporate body or legal entity, which is authorised to process personal data on behalf of the data controller.

Processing of personal data: an operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as access to, obtaining, collection, recording, structuring, storage, adaptation or alteration, retrieval, reconstruction, concealment, consultation, use, disclosure by transmission, sharing, transfer, or otherwise making available, sale, restriction, erasure or destruction.

Distinguishing a data controller and a data processor

A data controller and a data processor have different roles and responsibilities. It is therefore important for organisations to carefully consider their roles, duties and obligations concerning their data processing activities, hence the need to distinguish between a data controller and and a data processor.

pwc

Data controller

If an entity decides on "why" and "how" someone's data should be processed, then such an entity is considered a data controller. To put it in context, employees whose job is to process the data of someone in an organisation would be doing so to fulfil the tasks of that organisation as a "data controller". Some practical examples include: collecting employee information for payroll purposes, using an online email service provider for promotional emails, providing online payment services or collecting the personal data of pupils and their guardians, clients or patients during an enrollment process. Therefore if an entity in Rwanda or outside Rwanda collects the data of individuals in Rwanda, then such an entity is required to register as a data controller at the National Cyber Security Authority (NCSA) through its Data Protection Office.

In addition, based on the definition of "data controller" under the Law, a data controller can jointly process personal data with another data controller. A joint controller relationship generally arises where two or more controllers jointly determine the purposes and means of the processing of personal data. Whereas the Law is silent on what a joint controller relationship is, we understand that the joint controller relationship arises where the joint controllers are processing personal data for the same purpose, or they are processing personal data for closely linked or complementary purposes. However, questions arise: who is responsible for reporting to the NCSA/ DPO? Who is responsible for compliance with the Law or who will be liable in case of a data breach or non-compliance with the Law? It is our view that both entities would be responsible for the compliance obligations and jointly liable in the case of any non-compliance with the Law.

Data processor

A data processor is usually a third party who is external to the company. A data processor only processes personal data on behalf of a data controller. The duties of the processor could include: perform payroll services; access to or consultation of a contacts database containing personal data; sending promotional emails; shredding documents containing personal data; posting or putting a photo of a person such as a student or employee on a website; or even storing the IP addresses of data subjects or video recording (CCTV). As is the case with data controllers, all data processors are required to register with the NCSA through the DPO.

Registration

As pointed out earlier, the Law requires those who intend to be data controllers or data processors to register with NCSA through its DPO before 15 October 2023 if they intend to continue lawfully handling personal data. This makes it almost mandatory for all entities registered in Rwanda — because in one way or another they hold personal data — to register with DPO. We note that the Law does not provide for registration thresholds and this lack of a registration threshold is likely to pose a great challenge, especially to small organisations who control or process personal data on a limited basis. Many jurisdictions with data protection laws have set thresholds to curb this challenge. For example, in Kenya data controllers and processors whose annual turnover is less than five million Kenyan Shillings (approximately USD40,000) and entities with less than ten (10) employees are not required to register with Kenya's Data Protection Office. We understand from the DPO that they plan to introduce thresholds in the near future, but for now all data controllers and processors are required to register with the DPO.

Registration procedure

Currently, registration as a data controller or a data processor is a manual process which requires the data controller and processor to download a form from the official DPO website, https://dpo.gov.rw/, then to complete and email it to the DPO. We however understand from the DPO that they are in the process of moving the registration to an online portal.

Requirements for registration

The registration requirements for a data controller and data processor are similar, apart from the data processor requirement to specify the contractual relationship with the controller. Thus, when registering, the person or entity who intends to act as a data controller or a data processor must indicate the following:

- The name and address of the applicant and its designated single point of contact.
- The name and address of the representative of the applicant, if one had been nominated by the applicant.
- A description of personal data to be processed and the category of data subjects.
- Whether or not the applicant holds or is likely to hold the types of personal data based on the sector in which they operate in.
- The purpose for which the personal data are to be processed.
- The categories of recipients to whom the data controller intends to disclose the personal data.
- The country to which the applicant intends to directly or indirectly transfer the data.
- The risks, in general, security measures and mechanisms to ensure the protection of the personal data.

Registration certificate

Upon meeting the requirements successfully, the data controller or data processor will be registered with the NCSA and they will also be issued a registration certificate by the NCSA through its DPO within 30 working days from the date of receipt of the application. It is important for data controllers and processors to note that it is the NCSA that determines the validity period of the registration certificate. There are no statutory fees such as registration or renewal fees.

Data controllers and processors have 15 working days following the date of issuance of their registration certificate to notify the NCSA through its DPO of any changes, and they have 45 working days before the expiry of their registration certificate to apply for a renewal. The Data Protection and Privacy Law also provides for mechanisms to cancel a registration certificate.

We understand that the DPO is set to put in place a register of data controllers and data processors, which they will keep, manage and update regularly. Businesses will be able to request to have their entry erased from the register. Individuals who wish to access the register of controller and processors will have to wait until the modalities for access to the register have been set by the NCSA/DPO.

Duties of a Data Controller and a Data Processor

- Data controllers and processors are expected to do the following:
- Implement appropriate technical and organisational measures.
- Keep a record of personal data and processing procedures.
- Carry out Data Protection Impact Assessments where the processing of personal data is likely to result in a high risk to the rights and freedoms of their data subjects.
- Perform such other duties as requested by the supervisory authority.

Personal Data Protection Officer (PDPO)

In addition, controllers and processors are required to designate a Personal Data Protection Officer (PDPO) who is in charge of liasing with other entities including the NCSA/DPO. Organisations are expected to publish the PDPO's contact information and communicate it to the NCSA/DPO.

A PDPO will be appointed by any organisations that process personal data, where the core activities of the organisation consist of data processing operations which require regular and systematic monitoring of data subjects or personal sensitive personal data (including sensitive personal data of convicts) on a large scale.

A group of companies may appoint one PDPO and a public authority may also have a single PDPO for several authorities or bodies. A PDPO could be a staff member of that organisation, but they must have the professional qualities to fulfil the duties of such a position. It is also advisable that this person be in a management or senior management position.

A PDPO has the following duties:

- To inform and advise the data controller, processor or third party of their obligations under this Law.
- To monitor compliance with this Law in the workplace including assignment of responsibilities, awareness-raising and training of staff involved in the processing operations and related audits.
- To provide advice where requested regarding the data protection impact assessment and monitor its performance.
- To cooperate with the supervisory authority and act as the contact point.

Data protection impact assessment (DPIA)

Under the Law, data controllers and processors will be required to undertake a data protection impact assessment ("DPIA") in certain circumstances as described below.

A DPIA is a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. Carrying out a DPIA is not mandatory for every personal data processing operation, it is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons". Such processing includes but is not limited to:

- Systematic and extensive evaluation of personal aspects relating to an individual which is based on automated processing, including profiling, and on which decisions are based that produce legal (or similarly significant) effects concerning the individual.
- Processing on a large scale of sensitive personal data.
- A systematic monitoring of a publicly accessible area on a large scale.
- Processing of personal data identified by the NCSA that is likely to result in a high risk to the rights and freedoms of natural persons.
- New technologies used to process personal data.

Based on the above, regular DPIAs are likely to be undertaken by certain types of entities, such as healthcare service providers, financial service providers, government entities, security companies, functional genomics companies, app developers/startups, marketing companies, IT companies, cloud service providers, and many more.

Penalties in relation to registration

Failure to register or report any change after receiving the registration certificate

A data controller or a data processor who fails to register or operate without a registration certificate or even fails to report a change after receiving a registration certificate commits an administrative misconduct, thus being liable to an administrative fine of no less than two million Rwandan francs (RWF2,000,000) (approximately USD2,000) but not more than five million Rwandan francs (RWF5,000,000) (approximately USD5,000). For corporate entities, one percent (1%) of the entity's turnover for the preceding financial year.

Providing false information

A data controller or data processor who provides false information during and after registration commits an offence which is punishable with imprisonment of not less than one (1) year but not more than three (3) years and a fine of no less than three million Rwandan francs (RWF3,000,000) (approximately USD3,000) but not more than five million Rwandan francs (RWF5,000,000) (approximately USD5,000) or one of these penalties.

How PwC Rwanda can help you become compliant

In assessing your requirements for registration and to help you prepare to register as a Data Controller or Processor, PwC Rwanda will support you as follows:

1. **Preparation of application.** We will assist you with the following:

a. Identifying the various categories of personal data processed by your organisation and distinguishing between sensitive personal data and general personal data.

b. Identifying the types of data subjects whose information is collected.

c. Identifying the purposes for which each category of personal data is collected.

d. Identifying and describing the risks, safeguards, security measures and mechanisms put in place to protect personal data and any steps taken to prevent unlawful use of personal data by the Data Controller or Processor.

2. **Complete Data Controller and/or Data Processor application:** We will assist you in completing your application for a data controller or data processor certificate.

3. **Policy suite:** Reviewing existing policies and making recommendations as to how they can be updated to comply with the Law. Identifying any other additional policies, procedures or guidelines that may be relevant.

4. **Data protection awareness and training:** To increase board, management and staff awareness of this Law and how it impacts the organisation and to highlight respective roles and responsibilities for managing data privacy risk so as to enhance the organisation's privacy culture.

5. **Application follow up:** Support in addressing any queries from the NCSA through its Data Protection Office regarding the application for registration.

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, Legal Business Services
joseph.githaiga@pwc.com
Joseph Githaiga

Paul Frobisher Mugambwa
Head of Tax and Fiscal Policy Leader
frobisher.mugambwa@pwc.com
Paul Frobisher Mugabwa

Caroline Kayondo
Senior Manager, Risk and Quality
caroline.kayondo@pwc.com
Caroline Kayondo

Kesly Kayiteshonga
Senior Associate,
Tax and Legal Business Services
kesly.kayiteshonga@pwc.com
Kesly Kayiteshonga

Tracy Odipo
Senior Associate,
Legal Business Services
tracy.odipo@pwc.com
Vivian Tracy O.

Kelvin Rwamushaija
Associate,
Tax and Legal Business Services
kelvin.rwamushaija.com
Rwamushaija Kelvin