

Data Protection in Rwanda

Data Protection Alert, October 2023



Background

The Data Protection Law (No. 058/2021 of 13/10/2021) came into effect on 15 October 2021 and became enforceable from 15 October 2023. Data controllers and processors who are already in operation must now conform to the provisions of this Law.

The Law applies to:

- The processing of personal data by electronic or other means;
- A data controller, a data processor, or a third party who:
 - is established or resides in Rwanda and processes personal data while in Rwanda;
 - is neither established nor resides in Rwanda, but processes personal data of data subjects located in Rwanda.

The National Cyber Security Authority (NCSA) has the overall mandate of supervisory authority on enforcing compliance, overseeing implementation of the Data Protection Law, guidance on application and carrying out investigations.

NCSA is yet to put in place regulations to guide in application of the Law. However, the Law lays down specific obligations that all Data controllers and Data processors must adhere to. There are stiff penalties imposed on non-compliance.





Obligations of The Data Controller and The Data Processor

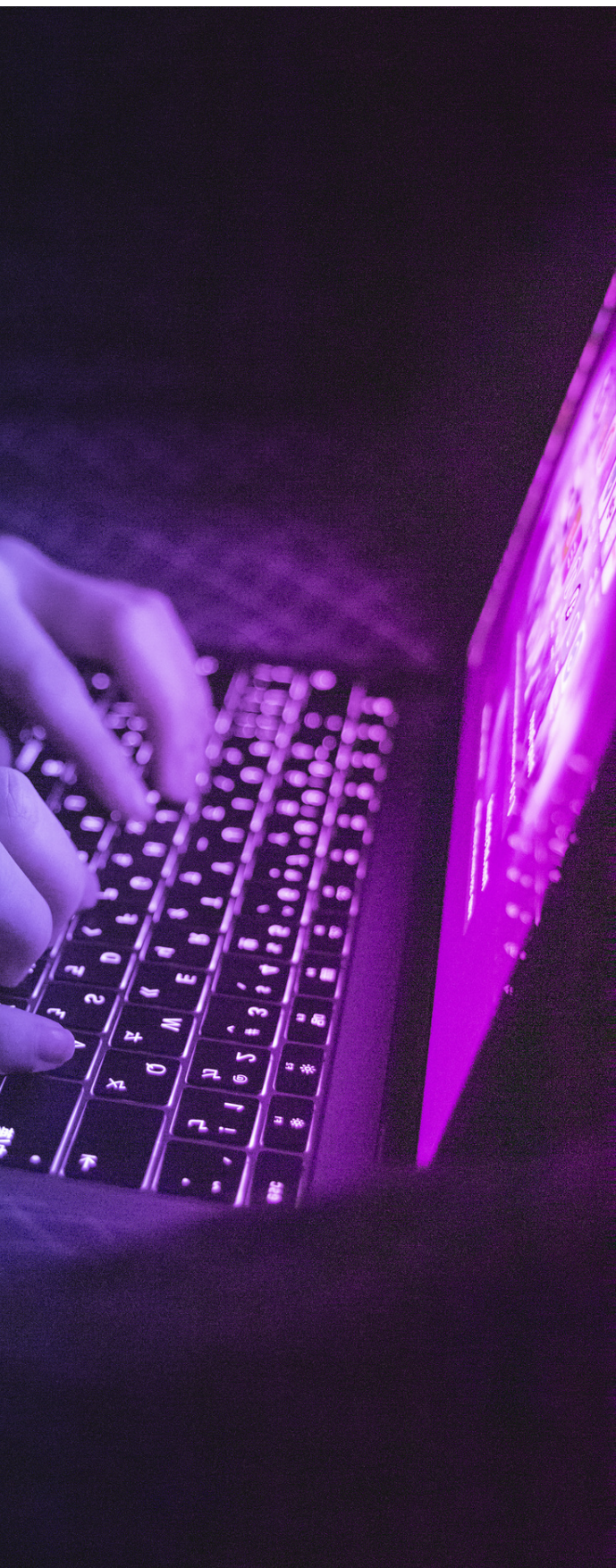
There are various obligations for the Data controllers and Data processors stipulated in the Law. In summary, those obligations are as follows;

- Registration with the Supervisory Authority;
- Adherence to data protection principles;
- Process personal data in a manner that respects the data subject rights;
- Maintain a log of personal data processing activities;
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the data subjects;
- Carry out personal data impact assessment where processing is likely to result in a high risk to the rights and freedoms of the data subject;
- Designate a representative in Rwanda where the entity is not established nor resides in Rwanda;
- Designate a data protection officer;
- Communication of data breach to Supervisory Authority/data subjects and submission of the incident report; and
- Obtain authorization from Supervisory Authority before transferring any data outside Rwanda.

REGISTRATION

Similar to other jurisdictions, the Data controllers and Data processors are required to register with the NCSA. Upon application and review, the NCSA will issue a registration certificate within 30 days of the application.

The validity period of the registration certificate is not yet determined.



Principles Of Personal Data Protection

The processing of personal data must be in accordance with the six principles of data protection that govern the processing of personal data. These include:

- **Lawfulness, Transparency, and Fairness:** The processing of data should be done lawfully, fairly, and in a transparently manner. Data controllers and Data processors must notify Data subjects of processing activities and obtain consent where necessary.
- **Purpose Limitation:** The personal data collected is only for explicit, specified, and legitimate purposes and is not further processed in a manner incompatible with the intended purpose.
- **Data Accuracy:** Personal data must be accurate and, where necessary, kept up-to-date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay.
- **Storage Limitation:** Personal data should be kept in a form that permits identification of data subjects for no longer than necessary for the purpose for which the data is processed.
- **Rights of Data Subjects:** The personal data is processed in compliance with the rights of data subjects.
- **Data Minimization:** The personal data being processed by the data controller or data processor must relate to the purposes for which the processing was requested.

Transfer of Data Outside Rwanda

Data controllers or Data processors must store personal data in Rwanda. Storage of personal data outside of Rwanda is only permitted if the Data controller or Data processor holds a valid registration certificate authorizing them to transfer or store personal data outside Rwanda.

The Data controller or Data processor transferring personal data outside of Rwanda must enter into a written contract with the transferee setting out the respective roles and responsibilities of each party to ensure compliance with the Data Protection Law.

A regulation from the NCSA determining the form of contract to be used for transfers of personal data outside Rwanda is yet to be issued.

Data Protection

The Data controllers and Data processors are required to ensure security of the personal data in their possession by adopting appropriate, reasonable technical and organisational measures to prevent loss, damage or destruction of personal data.

The Data Protection Law also requires Data controllers or Data processors processing sensitive personal data are required to implement appropriate safeguard measures including storing sensitive personal data separately from other types of data or applying measures such as tokenization, pseudonymization or encryption.



Breach Notification

In case of personal data breach, the Data controller is required to communicate the personal data breach to the NCSA within 48 hrs after being aware of the incident and file a report of the incident within 72 hours. A Data processor is required to notify the Data controller of any personal data breach within 48 hrs after being aware of the incident.

The NCSA can request the Data controller to notify the Data subjects if the Data controller has not done it yet in case the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject.

Offences, Administrative Fines and Penalties

The Data Protection Law provides for administrative misconduct sanctioned by administrative fines (Article 53) and offences sanctioned by imprisonment and fines (Article 56 to 63).

Offence	Penalty
Administrative misconduct: <ul style="list-style-type: none"> Operating without a registration certificate, Failure to designate a personal data officer, Failure to respect obligations related to personal data breach (notification, report, and communication) (Article 53). 	An administrative fine of not less than two million Rwandan francs (RWF 2,000,000) but not more than five million Rwandan francs (RWF 5,000,000) or one percent (1%) of the global turnover of the preceding financial year.
Processing personal data in a way that is contrary to the Data Protection Law including re-identification of de-identified personal data contrary to the Data Protection Law.	Imprisonment of not less than one (1) year but not more than three (3) years and a fine of not less than seven million Rwandan francs (RWF 7,000,000) but not more than ten million Rwandan francs (RWF 10,000,000) or one of these penalties.
Destruction, erasure, concealment or alteration of personal data contrary to the Data Law Protection Law.	Imprisonment of not less than three (3) years but not more than five (5) years and a fine of not less than seven million Rwandan francs (RWF 7,000,000) but not more than ten million Rwandan francs (RWF 10,000,000) or one of these penalties.
Sale of personal data contrary to the Data Protection Law.	Imprisonment of not less than five (5) years but not more than seven (7) years and a fine of not less than twelve million Rwandan francs (RWF 12,000,000) but not more than fifteen million Rwandan francs (RWF 15,000,000) or one of these penalties.

Offence	Penalty
Collection or process of sensitive personal data contrary to the Data Protection Law.	Imprisonment of not less than seven (7) years but not more than ten (10) years and a fine of not less than twenty million Rwandan francs (RWF 20,000,000) but not more than twenty-five million Rwandan francs (RWF 25,000,000) or one of these penalties.
Provision of false information.	Imprisonment of not less than one (1) year but not more than three (3) years and a fine of not less than three million Rwandan francs (RWF 3,000,000) but not more than five million Rwandan francs (RWF 5,000,000) or one of these penalties.
Sending unsolicited commercial communication to customers.	An administrative fine of between RWF 50,000 and RWF 500,000.
Spamming - sending of unsolicited messages repeatedly or to a large number of persons by use of a computer.	An imprisonment term of 3 months to 6 months and a fine of RWF 300,000 to RWF 500,000.

Corporate body or legal entity convicted of committing offence(s) is liable to a fine amounting to 5% of the annual turnover of the previous financial year (Article 62).

Additional penalties for the offences that the court can order include (Article 63):

- Seizure or confiscation of items used in the commission of any of the offences; and
- Permanent or temporary closure of the legal entity or body or the premises in which any of the offences were committed.

How Can PKF Help?

We understand the importance of data privacy, the legislation and regulations around it, the best practices to safeguard and protect personal data and ultimately demonstrate compliance with the laws.

We can assist as follows:

- Performing data protection legislation and regulation compliance audits;
- Advising and train on the implementation roadmap to achieve compliance with the laws;
- Conducting an inventory of personal data held by data handlers;
- Risk assessment and data protection impact assessment;
- ICT audit to assess the effectiveness of information security policies, procedures and information system controls in place;
- Advisory on remediation of known or identified gaps;
- Awareness training; and
- Application for registration with the supervisory authority.



Contact Persons:



Eric Njuguna
Managing Partner - Rwanda
enjuguna@rw.pkfea.com
+250 786 915 197



David Nzioki
Director - Audit
dnzioki@rw.pkfea.com
+250 787 169 273



Hezekiah Kamau
Director - Risk Management
hndungu@ke.pkfea.com
+254 720 257 266

Alternatively, you may contact or visit our office located at the address below:

KG 5 Avenue 44 , Kacyiru
P. O. Box 341,
Kigali, Rwanda
Tel: +250 788 386 565, +250 788 454 746
E-mail: pkfkgl@rw.pkfea.com

DISCLAIMER

The information provided here is intended as guidance and should not be considered a replacement for professional advice. Although we have taken every effort to ensure the accuracy of the information, PKF Consulting (R) Limited, its directors, or associates cannot be held responsible for any actions taken without seeking appropriate professional advice.

PKF Rwanda is a member firm of the PKF International Limited family of legally independent firms and does not accept any responsibility or liability for the actions or inactions on the part of any individual member or correspondent firm or firms.