DATA PROTECTION LAWS OF THE WORLD

Rwanda

RWANDA

Last modified 17 January 2024

LAW

The law governing data protection in Rwanda is the Law n°058/2021 of 13/10/2021 relating to the protection of personal data and privacy (the “**Data Protection Law**”).

Data Protection Law came into effect 15th October 2021. Data controllers and processors who are already in operation have a period of two (2) years from the Data Protection Law commencement date to conform to its provisions.

The Law n° 24/2016 of 18/06/2016 governing Information and Communication Technologies in Rwanda (the “**ICT Law** ”).

The Law n° 60/2018 of 22/8/2018 on prevention and punishment of cyber-crimes (the “**Cyber Crime Law**”).

DEFINITIONS

Definition of Personal Data

The Data Protection Law defines personal data as *“any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as:*

- *name*
- *identification number*
- *location data*
- *an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person”* (article 3, 1°).

Definition of Sensitive Personal Data

The Data Protection Law defines sensitive personal data as *“information revealing a person’s race, health status, criminal records, medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life or family details”* (article 3, 2°).

NATIONAL DATA PROTECTION AUTHORITY

The supervisory authority regarding Data protection is the National Cyber Security Authority (“**NCSA**”) (article 3, 23°).

REGISTRATION

A Data Controller is defined as a *“natural person, public or private corporate body or legal entity which, alone or jointly with others, processes personal data and determines their means of their processing”* (article 3, 19 °).

A Data Processor is defined as a *“natural person, public or private corporate body or legal entity, which is authorised to process personal data on behalf of the data controller”* (article 3, 24°).

Data controllers (“**DC**”) and Data Processors (“**DP**”) are required to register with the NCSA. (article 29).

The registration application must indicate the following (article 30):

- identity of the DC or DP and their designated single point of contact;
- identity and address of their representative if they have nominated any;
- 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 sectors in which it operates;
- purposes of the processing of personal data;
- categories of recipients to whom the DC or DP intends to disclose the personal data;
- country to which the applicant intends to directly or indirectly transfer the personal data; and
- risks in the processing of personal data and measures to prevent such risks and protect personal data.

The NCSA issues a DC or DP registration certificate within 30 days of the application.

A regulation from the NCSA determining the validity period of the registration certificate is yet to be adopted (article 31).

DATA PROTECTION OFFICERS

The Data Protection Law requires that the DC and DP designate a data protection officer in the following cases (article 40):

- the processing of personal data is carried out by public or private corporate body or a legal entity, except courts;
- the core activities of the DC or the DP consist of personal data processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- the core activities of the DC or the DP consist of processing on a large scale of sensitive personal data and personal data of convicts in accordance with the Data Protection Law’s requirements for the process of such data.

COLLECTION & PROCESSING

The DC is required to only collect personal data for a lawful purpose connected to its the activity and when the data is necessary for that purpose (article 42).

When collecting personal data, the DC is required to inform the data subject of the following:

- identity and contact details;
- purposes for which personal data are collected;
- recipients of such personal data;
- whether the data subject had the right to provide personal data voluntarily or mandatorily;
- the existence of the right to withdraw consent at any time and that such withdrawal does not affect the lawfulness of the processing of personal data based on consent before its withdrawal;
- the existence of the right to request from the DC access and ratification, restriction or erasure of personal data concerning the data subject or to object to the processing of the data;
- the existence of automated decision-making including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing personal data for the data subject;
- the period for which personal data will be stored;
- the right to appeal to the supervisory authority;

- where applicable, that the DC can transfer personal data outside of Rwanda and assures the data subject of the personal data security;
- any further information likely to guarantee fair processing of the personal data, having regard to the specific circumstances in which the data are collected.

The DC is not subject to the above disclosure requirements if:

- the data subject already has the information;
- the provision of such information proves impossible or involves a disproportionate effort; or
- the recording or disclosure of the personal data is required by the Data Protection Law.

The DC or DP must handle personal data for lawful purposes which include the following (article 46):

- the data subject’s consent to process their personal data for purpose explained to them;
- processing is necessary:
    - for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - for the execution a legal obligation to which the DC is subject;
    - for the protection of vital interests of the data subject or any other person;
    - for the performance of a duty carried out in the public interests or in the exercise of official authority vested in the DC;
    - for the performance of duties of a public entity;
- the processing is intended for legitimate interests pursued by the DC or by a third party to whom the personal data are disclosed, unless the processing is unwarranted in any particular case having regard to the prejudice to the rights and freedoms or legitimate interests pursued by the data subject;
- the processing is carried out for research purposes upon authorization by relevant institution.

The Data Protection Law also provides for requirements relating to the processing of personal data of a child under the age of 16 years which include the following (article 9):

- processing of the child’s personal data is subject to obtaining the consent of the holder of parental responsibility over the child;
- the consent obtained on behalf of the child must be given in the child’s interest to be acceptable;
- the consent is not required if it is necessary for protecting the vital interest of the child.

The DC or DP must store personal data in Rwanda. Storage of personal data outside of Rwanda is only permitted if the DC or DP holds a valid registration certificate authorising them to transfer or store personal data outside Rwanda (article 50).

TRANSFER

The transfer of personal data outside of Rwanda is only permitted for the following cases (article 48):

- the DC or DP has obtained authorization from the NCSA after providing proof of appropriate safeguards with respect to the protection of personal data;
- the data subject has given his or her consent;
- the transfer is necessary:
    - for the performance of a contract between the data subject and the DC or the implementation of a pre-contractual measures taken in response to the data subject’s request;
    - for the performance of a contract concluded in the interest of the data subject between the DC and a third party;
    - for public interest grounds;
    - for the establishment, exercise, or defense of a legal claim;
    - to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving his or her consent;
    - for the purpose of compelling legitimate interests pursued by the DC or by the DP, which are not overridden by the interests, rights and freedoms of the data subject and when:

- transfer is not repetitive and concerns only a limited number of data subjects;
- the data controller or the data processor has assessed all the circumstances surrounding the data transfer and has, on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data;

- for the performance of international instruments ratified by Rwanda.

The DC or DP 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 (article 49).

A regulation from the NCSA determining the form of contract to be used for transfers of personal data outside Rwanda is yet to be adopted (article 49).

SECURITY

The DC and DP are required to ensure security of the personal data in their possession by adopting appropriate, reasonable technical measures to prevent loss, damage or destruction of personal data which include the following (article 47):

- identify foreseeable risks to personal data under that person’s possession or control, establish and maintain appropriate safeguards against those risks;
- regularly verify whether the personal data safeguards are effectively implemented;
- ensure that the personal data security safeguards are continually updated in response to new risks or any identified deficiencies.

The NCSA is entitled by the Data Protection Law to conduct inspection and assessment of these security measures.

The Data Protection Law also provides for safeguards that DC or DP processing sensitive personal data must adopt including storing sensitive personal data separately from other types of data or applying measures such as tokenisation, pseudonymisation or encryption (article 11).

BREACH NOTIFICATION

In case of personal data breach, the DC is required to communicate the personal data breach to the NCSA within 48h after being aware of the incident. The DP is required to notify the DC of any personal data breach within 48h after being aware of the incident (article 43).

Where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, the DC is also required to communicates the personal data breach to the data subject in writing or electronically, after having become aware of it (article 45). The Data Protection Law does not specify in which delay this communication must be done.

This communication of personal data breach to the data subject is not required in the following cases:

- the DC has implemented appropriate technical and organisational protection measures in relation to personal data breached such that the personal data breach is unlikely to result in a high risk to the rights and freedoms of the data subject;
- the DC has taken measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialize;
- the DC communicated it to the public whereby the data subject is informed in an equally effective manner.

The NCSA can request the DC to make such communication if the DC 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.

ENFORCEMENT

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).

The administrative fines related to administrative misconduct imposed by the NCSA include 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). The administrative fine is between RWF 2,000,000 to RWF 5,000,000 or 1% of the global turnover of the preceding financial year for corporate body or legal entity.

Any person not satisfied with the administrative sanction taken against them has the right to file an application to the competent court (article 54).

The NCSA is the initial organ in charge of settlement of conflicts arising in relation to the Data Protection Law.

The Data Protection Law provides that the following violations are considered criminal offences (article 56 to 61):

- access, collection, use, offer, share, transfer or disclosure of personal data contrary to the Data Protection Law;
- re-identification of de-identified personal data contrary to the Data Protection Law;
- destruction, erasure, concealment or alteration of personal data contrary to the Data Law Protection Law;
- sale of personal data contrary to the Data Protection Law;
- collection or process of sensitive personal data contrary to the Data Protection Law;
- provision of false information.

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;
- permanent or temporary closure of the legal entity or body or the premises in which any of the offences were committed.

ELECTRONIC MARKETING

The Data Protection Law provides for the data subject right to object to the processing of his/her personal data for direct marketing purposes including profiling to the extent that it is related to such direct marketing (article 19).

The ICT Law provides that a person who sends unsolicited commercial communications to a consumer, provides the consumer with the option to cancel the subscription to the mailing list of that person and identify particulars of the source from which that person obtained the consumer's personal information, upon the request of the consumer (article 168).

The ICT Law also provides that a person is not allowed to transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by means of electronic mail where (article 223):

- the identity of the person who has sent the communication has been disguised or concealed;
- an address to which the recipient of the communication may send a request that such communication ceases has not been provided.

Sending unsolicited commercial communication to consumer is sanctioned by an administrative fine of between RWF 50,000 and RWF 500,000.

The Cyber Crime Law establishes spamming as a criminal offence (article 37). The Cyber Crime Law defines spamming as any intentional and without authorisation from a competent organ sending of unsolicited messages repeatedly or to a large number of persons by use of a computer or a computer system. Spamming also include the use of a computer or a computer system, after receiving a message, to retransmit such a message to many persons or retransmit it several times to a person who doesn’ t need it.

The penalties for this offence are an imprisonment term of 3 months to 6 months and a fine of RWF 300,000 to RWF 500,000 (article 37).

The prosecution of spamming offence is however instituted only upon complaint of the offended person (article 37).

ONLINE PRIVACY

The Data Protection Law provides that the DC, DP or third-party processing personal data must respect the privacy of the data subject (article 5). It does not provide any other specific requirement regarding cookies and location data.

KEY CONTACTS

Moses Kiiza Gatama
Senior Partner
T +250 788 303 877
moses.kiiza@equityjuris.com

Ian Mulisa
Partner
T +250 788 678 515
ian.mulisa@equityjuris.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.