Data Protection Alert

A general overview of the Rwanda Data Protection and Privacy Law

January 2023

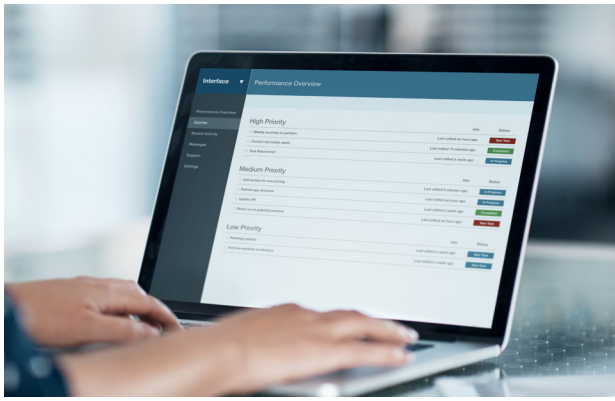
This alert forms part of a three-part series on Rwanda's personal data protection and privacy law. The next publications will cover the registration and duties of data controllers/processors which will be followed by an alert on the storage and transfer of personal data according to the Law relating to the Protection of Personal Data and Privacy (N° 058/2021 of 13/10/2021).

Personal data has been dubbed 'the new oil', mainly because personal data today drives a number of businesses through personalised customer experiences or even automated marketing messaging. This excessive collection of personal data by companies has created a lack of access control and has exposed individuals to risks such as fraud.

Hence, Rwanda saw a need to introduce a data protection law with the measures and safeguards recognised by other data privacy instruments such as the General Data Protection Regulation (GDPR) to ensure the protection of personal data collected in Rwanda. One could also argue that this Law was introduced to increase Rwanda's attractiveness as a new and modern international financial centre on the African continent.

In terms of applicability of the Law, the Law came into force the day it was gazetted on 15 October 2021, but in order to allow entities that collect and process data to prepare and register with National Cyber Security Authority (NCSA) the Law is to become operational on 15 October 2023 — after two years. So those who collect or process personal data of individuals in Rwanda have until 15 October 2023 to register at the National Cyber Security Authority.

As more and more social and economic activities take place online, the importance of privacy and data protection is increasingly



recognized. The Rwanda Protection of Personal Data and Privacy Law aims at protecting this fundamental right to privacy by regulating the processing of personal data, providing individuals' rights over their data, and setting up systems of accountability and obligations for those who process personal data.

As Rwanda joins the rest of the world in the protection of the right to privacy in this digital age, organisations who collect and process personal data in sectors like banking, insurance, healthcare, hospitality, education and non-profit will see themselves fall under the purview of this Law.

This Law consists of regulating the processing of personal data done by electronic means or other means. It also provides grounds for collecting and processing personal data, safeguards the requirements for the processing of personal data including sensitive data and the general

Organisations who collect and process personal data in sectors like banking, insurance, healthcare, hospitality, education and non-profit will see themselves fall under the purview of this Law

pwc

rules applicable for collecting and processing personal data. It also provides the right of data subject and punishment for failure to comply with the requirement of the Law by data controllers and data processors.

The scope and application of the Rwanda Privacy Law

The Law applies to the processing of personal data by any data controller, data processor or a third party who is established or resides in Rwanda and processes personal data while in Rwanda. In addition, this Law has an extra territorial applicability of its scope — it sets out that the Rwanda Data Privacy Law will still apply to a data controller, data processor or a third party who may not reside or be established in Rwanda but processes personal data of data subjects located in Rwanda.

Principles of personal data protection

Under this Law, there are six principles governing the processing of personal data. These principles are set out as obligations of data controllers and data processors. At a glance, these are the principles of personal data protection:

1. **Lawfulness and fairness:** This refers to processing of personal data which must be done in a lawful, fair and transparent manner.
2. **Rights of Data Subjects:** This refers to processing of personal data in accordance with the rights of data subjects.
3. **Purpose Limitation:** Personal data is collected only for a specific, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes.
4. **Data Minimization:** Personal data must relate to the purposes for which the processing was requested. This principle requires a data controller or data processor to limit the collection of personal data to what is directly relevant and necessary to accomplish a specific purpose.
5. **Data Quality:** 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.
6. **Storage Limitation:** Personal data must be kept in a form which permits identification of a data subject for no longer than is necessary for the purposes for which the personal data is processed.

Lawful processing of personal data

Rwanda's Data protection and Privacy Law sets out various lawful bases for processing personal data. Personal data can either be processed where consent is given by the data subject, or where processing is necessary under various circumstances including compliance with any legal obligation by the data controller/data processor or the performance of a contract to which the data subject is a party.

A data controller or data processor is considered to have processed personal data lawfully if:

- There is consent from the data subject to process his or her personal data after the data controller or data processor has explained the purposes for processing to the data subject;
- The processing is necessary for the performance of a contract to which the data subject is a party or the processing is part of steps to be taken prior to entering a contract;
- The data controller executes a legal obligation to which he is a subject;
- It is for the protection of the vital interests of the data subject or any other person;
- It is necessary for the public interest reasons or in exercise of official authority given to the data controller;
- It is for the performance of duties of a public entity;
- It is intended for legitimate interests which are pursued by the data controller or a third party to whom the personal data is disclosed; or
- It is carried out for research purposes with authorization of the relevant institutions.

Rights of data subjects and obligations of data controllers/ processors

The Rwanda Data protection and Privacy Law imposes positive obligations on data controllers and data processors to comply when processing personal data.

The Law provides the following rights to data subjects:

Data subject's right	Data controller or data processor duty
Right to withdraw consent to data collection or processing.	The data controller or data processor has a duty to cease collecting or processing the subject's data when the consent is withdrawn.
Right to information: The Law provides for the right of the data subject to request the data controller or data processor information relating to purposes of processing their personal data, a description of the personal data that the controller or processor holds, including data on third parties or categories of third parties who have access to the data subject's data.	The data controller or data processor has a duty to avail any information requested by the data subject in a clear and concise manner.
Right to object: A data subject has the right to object to processing of personal data which causes or is likely to cause loss, sadness, or anxiety to the data subject. However, this right is not absolute. the right to object will be set aside if the data controller or data processor provides compelling grounds for the processing which override the interests, rights and freedoms of the data subject or if it is for the establishment of a legal claim.	The data controller or the data processor has a duty to stop processing personal data at the request of the data subject if the processing causes or is likely to cause the data subject loss, sadness or anxiety, or if the data processed is used for direct marketing purposes such as profiling. The data controller or data processor must respond to the data subject's objection within 30 days of receipt with a written response of compliance and request or reasons for non-compliance, if any.
Right to personal data portability: The data subject has a right to request the data controller to present the personal data concerning him or her in a structured and machine-readable format. The data subject has a right to request the data controller to have his or her personal data transmitted to another controller, where technically feasible.	The data controller has a duty to provide the data subject with the requested personal data within 30 days of receipt of the request. The data controller has a duty to transfer the data subject's personal data to another data controller, provided it is technically feasible.
Right to not be subject to a decision based on automated data processing: The data subject has a right not to be subjected to a decision based solely on automated personal data processing including profiling which may produce legal consequences to him or her. However, this right is not absolute. The data subject will not be able to exercise this right if: • the decision is based on his/her consent, • it is necessary for entering into, or performance of, a contract between the data subject and controller, or • It is authorised by law and the Law puts in place suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.	The data controller or the data processor has a duty to comply with requests to reconsider an automated decision or take a new decision that is not based solely on automated processing, provided the decision does not fall within the three exceptions listed on the left.
Right to restrict processing of personal data, unless it is necessary for the protection of the rights of others, or for public interest: The Law prescribes for restriction of processing of a data subject's personal data. This may be enforced by the data subject themselves or NCSA for a given period of time.	The data controller has a duty to stop the processing of personal data of the data subject. The data controller or data processor has a duty to notify the data subject in writing or electronically if he is unable to lift the restrictions in order to protect the rights of others.
Right to erasure: The data subject has a right to request the data controller or data processor to erase all of the data they hold on him/her. However, this right is not absolute. This right does not apply if the processing is necessary for public interest reasons, for historical or scientific research purposes, for compliance with legal obligation, or for the establishment, exercise or defence of legal claims in the interest of the data controller.	The data controller has a duty to erase the data subject's personal information, within 30 days of receipt of the data subject's request. The data controller has a duty to take all reasonable steps to inform third parties processing the data subject's personal data of the request for erasure.
Right to rectification: The data subject has a right to request a data controller for correction of his or her personal data. This may be in regards to personal data which is incomplete and the data subject requests for its rectification from the data controller to capture the correct details.	The data controller has a duty to correct inaccurate personal data within 30 days of receipt of the data subject's request and must inform the data subject of the rectification.
Right to designate an heir to personal data: Unlike other privacy laws such as the GDPR, this Law introduces the concept of succeeding personal data of a deceased data subject, in circumstances where the data subject left a will. In such a case, the heir of the deceased data subject has the full or restricted rights relating to the processing of personal data kept by the data controller or data processor, if such personal data still needs to be used.	If the data subject provides an heir in his will, with full or restricted rights relating to the processing of the personal data kept by the controller or processor, provided such data still needs to be used, then the data controller or processor has a duty to respect the instructions that the data subject has left in their will in relation to the processing of the personal data kept by the controller or processor.

Duties and powers of the National Cyber Security Authority

The Government of Rwanda passed Law No 26/2017 of 31/05/2017 establishing the National Cyber Security Authority which was operationalised at the end of 2020. In addition, the law N° 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy designated NCSA as a supervisory authority with a duty to oversee its implementation which in turn created the data protection office (DPO) that is set out to lead on activities that ensure protection of personal data and guarantee the privacy of individuals in Rwanda of whose duties are listed in the table below.

Duties of the DPO	Powers of the DPO
Oversee the implementation of this Law.	Issue registration certificates as provided for by this Law.
Respond to every legitimate request for an opinion regarding personal data processing.	Ensure that the processing of personal data is consistent with the provisions of this Law.
Inform the data subject, controller, processor and third party of their rights and obligations.	Ensure that information and communication technologies do not constitute a threat to public freedoms and the privacy of a person.
Put in place a register of data controllers and data processors.	Put in place regulation relating to the application of this Law.
Investigate the subject matter of the complaint lodged by the data subject, controller, processor or third party and inform them of the outcome of the investigation within a reasonable period.	Impose administrative sanctions in accordance with the provisions of this Law.
Receive and consider the data subject's appeal.	
Advise on matters relating to the protection of personal data and privacy.	
Cooperate with authorities, organisations or entities operating within the country or abroad in the protection of personal data and privacy.	

Personal data breach

In case of a personal data breach, the data processor has forty-eight (48) hours after being aware of such breach to notify the data Controller.

In addition, the data controller must submit a report within seventy-two (72) hours of the breach, containing:

- The nature of the data breach,
- The contact details of the Personal Data Protection Officer (PDPO),
- Measures taken to mitigate the breach and its possible adverse effects,
- Facts relating to the personal data breach and remedial actions,
- Proposed communication of the breach to affected data subjects, unless the organisation has put in place appropriate technical and organisational measures such that the breach is unlikely to infringe on the rights and freedoms of the data subject, or if measures have been taken to ensure that the breach does not materialise, or the organisation already communicated the breach to the public at large whereby the data subject is informed as well.

Misconduct, offences and applicable penalties

A data controller, processor or third party who commits the following administrative misconducts will be liable for a fine between RWF 2,000,000 and RWF 5,000,000 or 1% of the company's annual turnover;

- Failure to maintain records of processed personal data;
- Failure to carry out personal data logging;
- Operating without a registration certificate;
- Failure to report a change after receiving a registration certificate;
- Using a certificate whose term of validity has expired;
- Failure to designate a personal data protection officer;
- Failure to notify a personal data breach;
- Failure to make a report on the personal data breach;
- Failure to communicate a personal data breach to the data subject.

A controller, processor or third party who is not satisfied with the administrative sanctions taken against them has a right to file an application to the competent court.

Offence	Penalty
Accessing, collecting, using, offering, sharing, transferring, or disclosing personal data in a way that is contrary to this Law.	Imprisonment of one to three years and a fine of RWF 7,000,000 to RWF 10,000,000, or one of these penalties.
Knowingly, intentionally, or recklessly re-identifying personal data which was de-identified by a data controller/processor or re-identifying and processing personal data without the consent of the controller.	Imprisonment of one to three years and a fine of RWF 7,000,000 to RWF 10,000,000, or one of the two penalties.
Unlawfully destroying, deleting, concealing, or altering personal data in a way that is contrary to this Law.	Imprisonment of three to five years and a fine of RWF 7,000,000 to RWF 10,000,000, or one of the two penalties.
Selling personal data in a way that is contrary to this Law.	Imprisonment of five to seven years, and a fine of RWF 12,000,000 to RWF 15,000,000, or one of the two penalties.
Collecting or processing of sensitive personal data in a way that is contrary to this Law.	Imprisonment of seven to ten years, and a fine of RWF 20,000,000 to RWF 25,000,000, or one of these penalties.
Providing false information.	Imprisonment of one to three years and a fine of RWF 3,000,000 to RWF 5,000,000, or one of these penalties.

A corporate body or legal entity that commits one of the offences mentioned in the table above will be liable, upon conviction, of a fine of 5% of its annual turnover of the previous financial year. In addition, the court may order the confiscation of items used in the commission of any of the offences. The court may also order permanent or temporary closure of the legal entity or body, or the premises in which any of the offences provided under this Law were committed.

Key definitions under the Rwanda Privacy Law

The following are the key definitions under the Rwanda Privacy Law explaining some key elements under the Law:

Personal Data: This means any information relating to an identified or identifiable natural person who can be identified directly or indirectly. Some practical examples include location data (GPS, or even the location data function on your mobile phone), an IP address, a cookie ID, or data held by your doctor (could be as far a symbol that uniquely identifies a patient).	**Data Subject:** The Law defines a Data Subject as a natural person from whom or in respect of whom, personal data has been requested and processed.
Data Controller: This means a natural person, a public or private corporate body or a legal entity which, alone or jointly with others, processes personal data and determines the means of their processing. Some entities that could fall under this category include healthcare service providers, telecommunication companies, schools, financial institutions, even those in the manufacturing sector. Government agencies including the tax authority, social security board, the police and other security agencies, the National Identification Agency, etc. As well as not-for-profit agencies such as charities, political parties,cooperatives, associations etc.	**Data Processor:** This means a natural person, a public or private corporate body or a legal entity, which is authorised to process personal data on behalf of the data controller. This includes payment processors, cloud storage providers,email marketing providers, marketing research firms, medical laboratories, business process and/or human resource outsourcing companies, government institutions such as the National Institute of Statistics of Rwanda (NISR), etc.
Data Processing: This means an operation or set of operations performed on personal data or on sets of personal data, whether by automated or manual processing means, by a data processor in accordance with the instructions of the controller based on a contract.	**Supervisory Authority:** This refers to the National Cyber Security Authority.
Sensitive Personal Data: Under the Rwanda Privacy Law, this means information revealing a person's race, health status, criminal or medical records, social origin, religious or philosophical beliefs, political opinion, genetic or biometric information, sexual life or family details.	**Personal Data Breach:** This means a breach of data security leading to unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Third Party: This means a natural person, a corporate body or legal entity other than the data subject, the data controller, the data pro-cessor and persons who, under the authority of the data controller, are authorised to process personal data.	**Vital Interest:** This refers to the interest linked to the life or death of the data subject.

How PwC Rwanda can help you become compliant

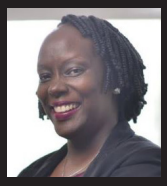
We can offer more detailed advice on issues arising under the Law and help your organisation on the following:

1. **Policy drafting –** we can assist your organisation with the drafting of a data privacy policy in line with the provisions of the Law. We can also review related documentation such as your contracts and standard terms and conditions and recommend amendments to align them with the Law.
2. **Readiness assessments –** we can help review your organisation's current data policies and practices in line with the provisions of the Law and international best practice. This will involve a multi-disciplinary team from PwC consisting of lawyers, risk professionals, forensic professionals and data technology professionals.
3. **Compliance roadmaps –** we can prepare a guideline for your organisation to assist you in the journey to compliance. Once again, this will involve a multi-disciplinary team from PwC to ensure your systems are compliant from all fronts.
4. **Implementation support –** we can assist your organisation with the implementation of the necessary changes to your data processing procedures. This will involve the mapping of data already held and redesigning the processes.
5. **Regulatory consulting –** we can provide regulatory advice services for your organisation on all general matters concerning data privacy.
6. **Training –** we can provide training to boards, management, and staff to sensitise them on their obligations under the Law.

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

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



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

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

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

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