Legal Alert

November 2023

The Rwanda Data Protection and Privacy Law provides for three grounds on which data controllers and data processors can rely on when transferring personal data outside of Rwanda: authorisation from the NCSA/ DPO, consent from the data subject or necessity. This article explores in detail how organisations operating in Rwanda can meet these requirements

Navigating cross-border data transfer: unveiling Rwanda's legal requirements

In our digitally interwoven world, the global flow of data is more vital than ever. However, this data flow comes with an inherent responsibility: ensuring that personal data remains shielded, respecting privacy and legal boundaries. Rwanda, too, stands at the forefront of this data ethics discourse with its stringent Data Protection and Privacy Law Nº 058/2021 of 13 October 2021 (the DPP Law). The DPP Law meticulously outlines the lawful processing of personal data and seeks to ensure its protection, not just within the borders of Rwanda, but also beyond.

This article sets out to explore a crucial dimension of the DPP Law, namely the transfer of personal data outside Rwanda. The DPP Law, recognizing the significance of global data exchange, provides specific guidelines and prerequisites for such transfers.

These prerequisites encompass authorization from the National Cybersecurity Authority (NCSA) through its Data Protection and Privacy Office (NCSA/DPO), robust safeguards to ensure data protection, and valid grounds for transfer such as explicit consent or fulfilling contractual obligations.

The complexities of this legal landscape demand a comprehensive understanding of the DPP Law's requirements. Therefore, we explore the legal requirements that govern the transfer of personal data beyond Rwanda. Each facet of compliance and every legal nuance will be unveiled, shedding light on how organisations can seamlessly and legally traverse the realms of cross-border data transfer, aligning their practices with the DPP Law.

Facilitating cross-border flow of personal data from Rwanda

The sharing and transfer of personal data outside Rwanda involve a nuanced framework, primarily summarised in three key avenues accessible to data controllers or processors.

1. **Authorization by NCSA/DPO, the supervisory authority.** The data controller or processor gains the ability to transfer personal data beyond Rwanda by securing authorization from the NCSA/DPO. This authorization is granted once substantiated evidence of robust safeguards ensuring the protection of personal data is presented.
2. **Consent from the data subject.** Another avenue for transfer is paved when the data subject expressly provides consent. This informed and unambiguous consent from the individual offers a valid pathway for data transfer.
3. **Necessity-based transfer.** Circumstances where data transfer is imperative present another dimension. Such necessity-driven transfers hold merit when they serve specific essential purposes, ensuring a lawful and justified sharing of personal data.

In the subsequent paragraphs, we explore each of these avenues in detail to unravel the intricacies and legal requisites for the secure and compliant sharing of personal data beyond Rwanda.

Authorisation by NCSA: Initiating the process of authorising personal data transfers beyond Rwanda

When transferring personal data outside Rwanda, organisations are required to obtain approval from the NCSA/DPO. This process involves the following:.

1. Procedure for authorization: Unveiling the implicit approach. Although the DPP Law does not explicitly delineate the procedure for obtaining approval to transfer personal data beyond Rwanda, the approach embraced by the NCSA/DPO has been indirectly implied through the registration certificate. This certificate clearly stipulates that data controllers and data processors must obtain valid authorisation from the NCSA/DPO for any transfer of personal data outside Rwanda.

   The NCSA/DPO facilitates this process by offering a dedicated application form for seeking authorisation to transfer personal data beyond Rwanda. This form is a comprehensive guide that details the step-by-step procedure for application, the legal basis underpinning the data transfer, the specific categories of personal data corresponding to various data subjects, and the countries receiving the personal data from Rwanda. Additionally, it entails an analysis of the personal data protection and privacy laws of the recipient countries, a risk assessment preceding the transfer, and the safeguards implemented by the data controller or data processor to fortify personal data protection.

2. Comprehensive documentation: The essential attachments. In support of the application for authorization, organisations are required to provide key privacy documents. A core inclusion is the Data Protection Impact Assessment (DPIA), which sets out a detailed assessment of privacy risks pertaining to the personal data marked for transfer, alongside the mitigating factors considered prior to the transfer. Furthermore, organisations must provide tangible evidence of existing contracts between the data controller or data processor in Rwanda and the entity slated to receive the personal data beyond Rwanda.

   i. Conducting a comprehensive Data Protection Impact Assessment (DPIA).

      This assessment entails a comprehensive examination of the system, technology or software responsible for hosting or storing the personal data earmarked for transfer.

      The DPIA is a rigorous analysis aimed at understanding the context of the personal data transfer and identifying potential risks associated with this process. It includes a risk rating for the identified risks and proposes measures to mitigate or eliminate these risks to safeguard the personal data effectively.

      The DPIA includes a description of the receiving entity's data protection framework and data security controls. This presentation of security measures highlights their commitment to ensuring the overall protection of personal data.

      When seeking authorization for personal data transfer outside Rwanda, a data controller or data processor must attach the DPIA to the application. This inclusion is instrumental in demonstrating to the NCSA/DPO that adequate safeguards are in place to mitigate any potential risks linked to the personal data destined for transfer.

   ii. Contracts. The other additional document required to be provided when submitting an application for authorisation to transfer personal data outside Rwanda is a contract or contractual agreements between the data controller and the data processor or third parties. This contract is called a data processing agreement. The DDP Law underscores the significance of a formal contract governing the transfer of personal data between a data controller or data processor and an involved third party. In essence, any intent to share or transfer personal data beyond Rwanda necessitates a well-defined, written contract with the third party. This contract serves as a foundational document, explaining the roles and responsibilities of each party concerning compliance with the Law's provisions when sharing personal data. A robust contract for personal data transfer must have pivotal details, including the following:

   - Identification of involved parties
   - Specification of the personal data being transferred
   - Clarification of the purpose behind the transfer
   - Outline of the security safeguards instituted by each party

   It's noteworthy that, while the DPP Law refrains from stipulating specific mandatory terms for inclusion in these contracts, organisations are strongly encouraged to align their contract terms with the principles and guidelines laid out in the DPP Law. This alignment ensures that the contracts uphold the essence and standards of data protection while enabling lawful data transfers.

Consent from the data subject

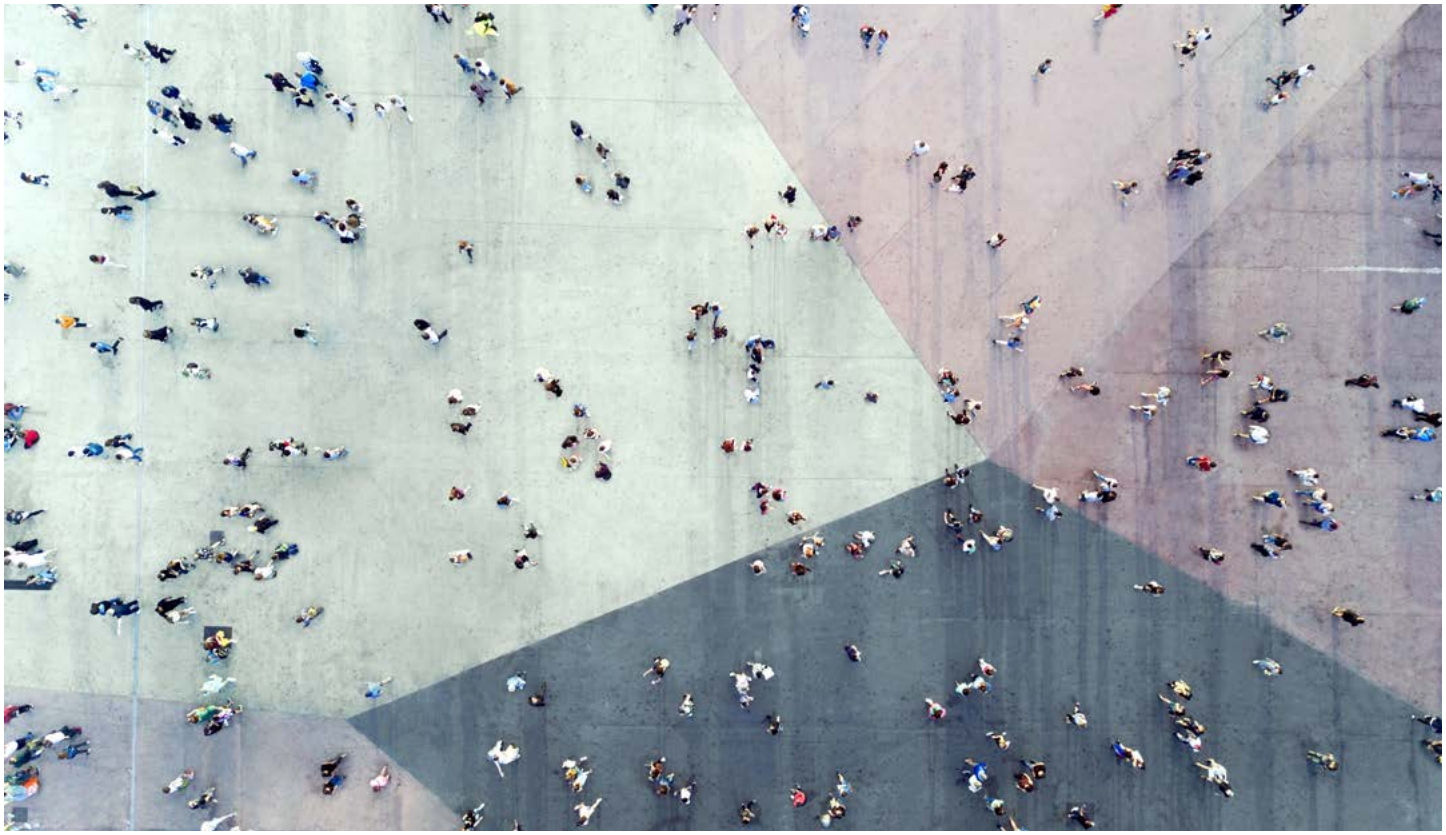
The second lawful ground for transferring personal data outside Rwanda hinges on the consent of the data subject. Here's a comprehensive breakdown:

1. Essence of valid consent. As outlined in the DPP Law, consent is a fundamental basis for lawful data transfer. However, for consent to hold legal weight, it must meet certain criteria. The data controller or data processor must demonstrate that the consent was willingly given, well-informed and unequivocal. Therefore, any data controller or processor intending to leverage consent as a basis for transfer must effectively communicate their intent to transfer the data subject's personal data to a specific jurisdiction, offering a clear rationale behind this decision.
2. Rigorous standards set by the DPP Law. The DPP Law sets a high standard for consent, emphasising that data controllers and processors must provide individuals with genuine choice and control. This entails employing a positive opt-in mechanism for consent, allowing data subjects to actively agree to the data transfer. Furthermore, data controllers and processors are obligated to grant data subjects the freedom to revoke their consent at any point. The withdrawal of consent should be as simple as the initial granting, and it should not affect the lawfulness of processing personal data based on consent before its withdrawal.
3. Empowering data subjects. In essence, this emphasis on consent seeks to empower data subjects, granting them the authority to make informed decisions regarding their personal data. Through clear communication, genuine choice and an easily accessible consent withdrawal process, the DPP Law ensures that data subjects retain control over their data even after it has been transferred.

Exploring necessity

A further basis for transferring personal data beyond Rwanda is necessity based on a set of specific grounds outlined in the DPP Law. These are explained below:

1. Contractual agreements with data subjects. A crucial facet of necessity arises when there exists a contract between the data controller and the data subject, or during pre-contractual measures initiated at the data subject's request. This scenario permits data transfer outside Rwanda to fulfil contractual obligations to the data subject or upon their specific request. One example lies in businesses conducting Know Your Client procedures that require data transfer for customer onboarding, especially when headquarters or partners are situated outside Rwanda. Another example is where an individual in Rwanda enters into a contract with an international e-commerce platform to purchase products. The platform, based outside Rwanda, needs to process and transfer the individual's personal data to fulfil the contract and deliver the purchased items.
2. Performing contract-related work that benefits data subjects. Another dimension of necessity occurs when the data controller transfers personal data in order to perform a contract concluded in the interest of the data subject, where the contract is between a data controller and a third party. For instance, when a data subject requires a service necessitating outsourcing from a third party or a party located beyond Rwanda. An illustrative instance could involve a Bank in Rwanda that subcontracts a third party debit card or credit card service provider located outside Rwanda. The third party card service provider will have access to the personal data of the customers of the local bank in Rwanda which shares the customer personal data in order to effect card transactions. The local bank would rely on the contract entered into between the local bank in Rwanda and the third party card service provider in order to effect card transactions between the bank and its customers.
3. Public interest grounds. Necessity is also invoked when transferring personal data based on public interest grounds. This scenario arises when the data controller establishes the necessity of transferring personal data outside Rwanda for the greater public interest. In a public health crisis like a global pandemic, health organisations worldwide may



need to share information about infected individuals. Rwandan health authorities might transfer personal data of affected individuals to global health bodies to ensure coordinated responses and research, a clear instance where public interest justifies data transfer without requiring authorization from the NCSA/DPO or consent from the data subject.

4. Legal claims. Necessity justifies data transfer when required for legal claims. If a data controller needs to assert or defend a claim against a data subject, sharing personal data outside Rwanda may become necessary, especially if the court or tribunal handling the case is situated outside Rwanda. Imagine a scenario where a Rwandan citizen is involved in a legal case against a multinational corporation. The Rwandan courts may require sharing the individual's personal data with the courts or legal entities in the corporation's home country to ensure a fair legal process.
5. Protection of vital interests. The law recognizes the necessity of sharing personal data to protect vital interests, either of the data subject or another person, particularly when the data subject is incapable of giving consent. For instance, in emergencies such as a work-related accident where immediate medical assistance is required outside Rwanda, the employer, acting as the data controller, can transfer personal data to facilitate medical insurance. In another instance, if a tourist meets with a severe accident while in Rwanda, the hospital treating them may need to share vital medical data with authorities in the home country of the tourist to coordinate necessary assistance and inform their family.
6. Compelling legitimate interests. In specific circumstances, necessity arises from compelling legitimate interests pursued by the data controller or processor, provided they are not outweighed by the interests, rights and freedoms of the data subject. A multinational company with a branch in Rwanda may need to transfer employee data to its global HR department for efficient management and payroll processing, ensuring the company's smooth operation. However, this can only apply when the transfer is not repetitive and concerns a limited number of data subjects. The data controller or processor must conduct a comprehensive assessment of the circumstances and implement suitable safeguards to protect personal data during the transfer.
7. Performance of international instruments: Lastly, the DPP Law allows for personal data transfer in accordance with international instruments ratified by the Rwandan government. This provision applies when Rwanda is a signatory to international treaties or agreements authorising personal data transfer within specified regions or groups of countries. By doing so, Rwanda ensures alignment with international agreements on data protection and privacy.

Ensuring compliance: Strategic steps for data transfer

In the pursuit of compliance, organisations must swiftly assess their current data processing practices to scrutinise data flows beyond Rwanda. This assessment is fundamental in identifying the necessary prerequisites before venturing into the transfer of personal data outside the country. It demands a flexible approach in selecting the appropriate lawful ground for the transfer. Here are the most important aspects for organisations to consider.

1. Identifying participation in cross-border transfers. A foundational step for data controllers and processors involves determining their involvement in cross-border transfers. This entails conducting a comprehensive data inventory to track the trajectory of personal data within the organisation. If an organisation exclusively collects personal data from individuals within Rwanda and does not share this information beyond the country, they fall outside the purview of cross-border transfer regulations.

2. Establishing a clear lawful basis. For organisations engaged in transferring personal data outside Rwanda, ensuring compliance with the DPP Law necessitates a transparent establishment of lawful grounds for the transfer. This involves identifying and documenting the legal justifications for the transfers. Whether it be obtaining consent, demonstrating necessity or relying on other legal grounds stipulated in the law, clarity in establishing the lawful basis is paramount.
3. Introducing enhanced data security measures. In the context of data transfer, fortifying data security measures is critical. Organisations should not only focus on legal compliance but also prioritise data protection. Implementing robust encryption, secure data storage practices and regular security audits can significantly enhance data security during transfers.
4. Prioritising data minimization and anonymization. Emphasising data minimization and anonymization is an evolving aspect of compliance. By reducing the volume of personal data shared and ensuring data is anonymized to the greatest extent possible, organisations can mitigate risks associated with cross-border data transfer and align with privacy principles.

> The DPP Law sets a high standard for consent, emphasising that data controllers and processors must provide individuals with genuine choice and control

5. Educating employees on data transfer compliance. Another proactive measure is to educate employees within the organisation about the intricacies of data transfer compliance. Training programmes and awareness initiatives can empower employees to handle personal data in a manner compliant with legal and ethical standards, reducing inadvertent violations.

Conclusion: Fostering responsible data transfer practices

In the ever-evolving landscape of data protection and privacy, the transfer of personal data beyond borders necessitates meticulous attention and a comprehensive understanding of legal foundations. Organisations must swiftly evaluate their data processing practices and discern their involvement in cross-border transfers. Clarity on the lawful basis for such transfers is paramount to ensure compliance with the DPP Law.

Business is becoming more data-centric, and we're seeing indispensable practices emerging in response.

These practices include bolstering data security measures, prioritising data minimization and anonymization, and imparting knowledge to employees. These steps not only foster compliance but also signify a commitment to responsible data handling.

In conclusion, proactive and strategic approaches are essential in the realm of data transfer compliance.

By aligning with legal requirements, reinforcing data security and prioritising ethical data practices, organisations can navigate the intricacies of cross-border data transfer to establish trust and uphold privacy in an increasingly interconnected world.

Stay committed to a responsible and ethical data journey to benefit individuals and society as a whole.

PwC Rwanda: Your trusted partner in achieving compliance

Navigating the intricacies of data protection laws, especially concerning the transfer of personal data, demands expert guidance. PwC Rwanda stands ready to support your organisation in achieving compliance through a spectrum of tailored services.

1. Streamlining the authorization process for data transfer

Our seasoned team of specialists can guide you through the intricate process of applying for authorization to transfer personal data outside Rwanda. From gathering the requisite information to preparing thorough documentation, we help you achieve a seamless application process. We also diligently monitor the application's progress and promptly address any inquiries from the NCSA/ DPO.

2. Ensuring adequate data protection with transfer impact assessments

We conduct transfer impact assessments to consider whether personal data remains adequately protected in the receiving entity located outside Rwanda. Through this assessment, we identify potential risks to personal data and recommend key measures your organisation can implement to mitigate these risks effectively.

3. Facilitating compliance with records of processing activity

The development of a record of processing activity (RoPA) is crucial for organisational transparency regarding personal data processing. Our experts assist in creating a RoPA by collating data inventories from key departments, ensuring your compliance with the DPP Law's requirements for data controllers.

4. Precision in data processing agreements

We offer support in crafting precise data processing agreements, which includes data sharing and data processing agreements. In adherence to the DPP Law, third-party data processing agreements are essential, and we provide standard templates tailored to your specific third-party engagements.

5. Comprehensive legal advisory

Understanding the legal landscape is fundamental in the compliance journey. Our legal experts are ready to advise your organisation on a myriad of legal matters related to data protection. We provide detailed and practical legal opinions tailored to your unique organisational structure.

6. Empowering through training and awareness

In collaboration with your organisation, we conduct training sessions to raise awareness among key staff members. Our aim is to sensitise boards, management and staff about their individual responsibilities in achieving overall compliance, with a particular focus on the nuances of personal data transfer.

Empower your organisation with PwC Rwanda's expertise for a smooth compliance journey and a culture of responsible data handling. Your trust in us propels you toward a future where compliance is seamless and data protection is paramount.

Contact us

Joseph Githaiga
Director
Head of Legal Business Solutions
joseph.githaiga@pwc.com

LinkedIn

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

LinkedIn

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

LinkedIn

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

LinkedIn

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

LinkedIn

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

LinkedIn