

PROCEDURE FOR TRANSFER OF PERSONAL DATA OUTSIDE NIGERIA

1. Background

Ringardas Nigeria Limited (“Ringardas” or the “company”) collects and processes Personal Data (**see Section 3 below**) such as name, address, mobile numbers, date of birth etc of individuals that makes them easily identifiable. Some of these individuals include current, past and prospective employees, suppliers/vendors or their representatives, customers and other individuals whom Ringardas communicates or deals with from time to time (“Data Subjects”).

In furtherance of the company’s business objectives, the company may transfer Personal Data out of Nigeria. The transfer of Personal Data of Data Subjects out of Nigeria is governed by specific requirements under the Nigeria Data Protection Regulation, 2019 (NDPR). To this end, Ringardas is firmly committed to complying with the provisions of the NDPR to ensure security of Personal Data handled by the company.

This document describes the minimum standards that must be adhered to by the company where Personal Data is to be transferred to a country outside Nigeria, in line with the NDPR.

2. Scope

This document applies to all employees of Ringardas as well as to any external business partners who process Personal Data received from Ringardas or on behalf of Ringardas.

3. Personal Data

Personal Data (as defined under the NDPR) means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.

4. Regulatory Procedure for Transfer of Personal Data Outside Nigeria

- 4.1. Where Personal Data is to be transferred to a country outside Nigeria, Ringardas shall put adequate measures in place to ensure the security of such Personal Data. In particular, Ringardas shall, among other things, conduct a detailed assessment

of whether the said country is on the National Information Technology Development Agency (NITDA) White List of Countries with adequate data protection laws (**See Appendix A**).

4.2. The transfer of Personal Data out of Nigeria would be in accordance with the provisions of the NDPR. Ringardas will therefore only transfer Personal Data out of Nigeria on one of the following conditions:

- a. The consent of the Data Subject has been obtained;
- b. The transfer is necessary for the performance of a contract between Ringardas and the Data Subject or implementation of pre-contractual measures taken at the Data Subject's request;
- c. The transfer is necessary to conclude a contract between Ringardas and a third party in the interest of the Data Subject;
- d. The transfer is necessary for reason of public interest;
- e. The transfer is for the establishment, exercise or defense of legal claims; and
- f. The transfer is necessary in order to protect the vital interests of the Data Subjects or other persons, where the Data Subject is physically or legally incapable of giving consent.

Provided in all circumstances, that the Data Subject has been manifestly made to understand through clear warnings, of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country. This proviso shall however not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

4.3. Where the recipient country is not on the White List and none of the conditions stipulated in Section 4.2 of this document is met, Ringardas will engage with NITDA and the Office of the Honourable Attorney General of the Federation (HAGF) for approval with respect to such transfer.

In such instances and in line with the provisions of the NDPR Implementation Framework, Ringardas will provide NITDA with the following information:

- a. A list of countries where the Personal Data of Nigerian citizens are transferred in the regular course of business;

- b. The Data Protection Laws and contact of National Data Protection Office/Administration of such countries where Personal Data is transferred to;
 - c. The privacy policy of Ringardas which is compliant with the provisions of the NDPR;
 - d. An overview of encryption methods and data security standards; and
 - e. Any other detail that assures the privacy of personal data is adequately protected in the target country.
- 4.4. Where Personal Data is transferred out of Nigeria pursuant to Section 4.3 above, Ringardas will work with NITDA to coordinate transfer requests with the office of the HAGF.

5. Transfer of Personal Data from Nigeria to other Entities within Ringardas

In addition to the procedure stated in Section 4 of this document, where Ringardas transfers Personal Data to any other entities within Ringardas, Ringardas will execute an Intra Group Transfer Agreement or a Third Party Processing Agreement with such company.

6. Disciplinary Actions

Failure to comply with the provisions of this document on procedure for transfer of Personal Data out of Nigeria which results in a violation of the NDPR is a material breach of Ringardas policies and may result in disciplinary action as required, including suspension or termination of employment or business relationship.

7. Contact for any Queries

Ringardas has appointed a DPO responsible for overseeing the Company's data protection strategy and its implementation to ensure compliance with NDPR requirements.

The DPO should be contacted if you have any queries or clarifications regarding the operation of this document. The contact details are set out below:

- Data Protection Officer- Patrick Ameh
- Phone - +234 8039828761

- Email: patrick.ameh@ascanigeria.com

8. Changes to this Policy

Ringardas reserves the right to change, amend or alter this document in line with any regulatory requirements or updates. If we amend this document, we will issue an updated version.

APPENDIX A**

SN	COUNTRY	SUMMARY OF LAW	REMARK
	All EU Countries	The GDPR principles apply and are adequate	Austria Belgium Bulgaria Croatia Cyprus Czech Republic Denmark Estonia Finland France Germany Greece Hungary Iceland Ireland Italy Latvia Lithuania Luxembourg Malta Netherlands Norway Poland Portugal Romania Serbia Slovakia Slovenia Spain Sweden United Kingdom
1	Angola	Data Protection Law (Law no. 22/11, 17 June 2011), the Electronic Communications and Information Society Services Law (Law no. 23/11, 20 June 2011) and the Protection of Information	DPL establishes <i>Agência de Proteção de Dados (APD)</i> as Angola's Data Protection Authority.

		Systems and Networks Law (Law no. 7/17, 16 February 2017).	
2	Argentina	Personal Data Protection Law 2000 (Law No. 25,326) applies to any person or entity in the country that deals with personal data.	National Authority: Agency for Access to Public Information established pursuant to Decree 746 of 2017
3	Australia	Federal Privacy Act 1988 is based on 13 APPs (Australian Privacy Principles) that cover transparency and anonymity; the collection, use and disclosure of data; maintaining the quality of data; and the data subject's rights. Australia has regional and sectoral privacy laws supplementing the FPA.	
4	Brazil	General Data Protection Law 2018 (LGPD) very similar to GDPR. Brazil also has snippets of privacy laws from the Constitution and other statutes such as Consumer Protection Code 1990; Internet Act 2014 etc.	The Amended LGPD created the National Data Protection Authority (ANPD). The law would take effect in August 2020
5	Canada	Private sector is governed by Personal Information Protection and Electronic Documents Act (PIPEDA) 2000 amended in 2008 to include mandatory data breach notification and record-keeping laws. the public sector is governed by the Privacy Act of 1983.	PIPEDA creates the Office of the Privacy Commissioner of Canada
6	Cape Verde	Data Protection Law (Law 133/V/2001 (as amended by Law 41/VIII/2013) and Law 132/V/2001, of 22 January 2001.	The National data protection authority in Cape Verde is the <i>Comissão Nacional de Proteção de Dados Pessoais</i> ('data protection authority').
7	China	Information Technology – Personal Information Security Specification is the latest law on privacy in China. It came into effect in May 2018	Cyberspace Administration of China (CAC) is the data protection authority in China

**** Please note that the list of countries in the NITDA's White List is subject to change and may be updated by NITDA from time to time. Where this is updated, the Company will reflect the update in this document.**

GENERAL INFORMATION

Title	Procedure for Transfer of Personal Data out of Nigeria
Status	Mandatory
Issuing Department	Data Protection Officer
Distribution/Target Audience	All employees, including contracted staff of Ringardas, vendors/suppliers of Ringardas, foreign third parties and the general public
Approver	Management of Ringardas Nigeria Limited
Effective Date	April 2021
Version	1.0

VERSION CONTROL

Version	Last Updated	Reason for Amendment