PAYSTACK INC.

Group in-house rules on the transfer of personal data

Binding Corporate Rules (BCRs)

Table of Contents

1) INTRODUCTION

Paystack Inc. and its subsidiaries (“Paystack”) are a leading fintech company, headquartered in Nigeria, with the parent company in America. Paystack provides innovative payment processing solutions, enabling African businesses to conduct over 500 million transactions globally with a team of more than 150 employees. Paystack operates across multiple countries and prioritises privacy and data security through a robust Data Protection Policy and Binding Corporate Rules (BCRs), ensuring compliance with global data protection laws and secure data storage on AWS servers in Ireland. This combination of technical expertise and stringent data governance highlights Paystack's commitment to empowering African commerce with trusted financial technology.

2) RULES APPLICABLE TO TRANSFER AND PROCESSING

Paystack Group's Binding Corporate Rules (BCRs) mandate that all internal transfers and processing of personal data across subsidiaries, employees, contractors, and temporary staff adhere to data protection principles. This includes lawful, fair, and transparent processing for specified purposes, secured by technical, organisational, and administrative safeguards. Processing must be based on legal grounds like consent or contractual necessity. Special conditions apply for sensitive data. Non-compliance is managed through existing contracts, and subsidiaries must meet local requirements while prioritizing the strongest applicable data protection laws. Where local laws fall short, Paystack will follow its BCRs to ensure consistent data protection.

3) INFORMATION AND TRAINING

Paystack keeps employees informed of BCRs and data protection policies via accessible internal documentation. Targeted training for Group Subsidiaries impacted by Data Transfer covers key principles, including onboarding, annual updates, role-specific modules, and assessments. Internal audits verify compliance and strengthen data protection.

4) GUARANTEES OF BCRs IMPLEMENTATION

4.1. Audits, Complaints procedure, Responsibility and Liability

Paystack Group conducts annual internal, external, and regulatory audits to ensure compliance with data protection policies and Binding Corporate Rules (BCRs). These audits review data processing, contractual obligations, safeguards, and third-party risk, with ongoing monitoring to identify and address any compliance gaps. Transparency is maintained through audit reports, feedback, and stakeholder meetings.

Additionally, Paystack has an independent complaints procedure for employees and data subjects. Local Data Protection Champions and Group HQ enforce BCRs, with subsidiaries accountable for breaches and liable for damages unless proven otherwise. The Group commits to remedial actions and compensation for breaches, ensuring strong accountability.

5) CONFLICTS OVER RULES

If a Subsidiary cannot apply these BCRs due to local law, it must contact its Local Data Protection Champion or the Group's Global Data Protection Office. They will decide on the necessary action, consulting Data Protection Authorities if unsure. Local laws providing higher personal data protection take precedence over the BCRs.

6) COOPERATION WITH THE COMPETENT AUTHORITIES

The Group commits to cooperating with the relevant Data Protection Authorities. This includes implementing their recommendations and advice, and responding to their requests concerning the BCRs, such as audit requests, within a reasonable timeframe.

7) COMPLIANCE WITH LAWS

Paystack promptly notifies Data Protection Authorities of personal data breaches as required by law. Group service providers act solely on data controller instructions, while maintaining proportional security measures. Paystack processes sensitive personal data only when necessary and with explicit consent, respects data subject rights (including marketing objections), records processing activities, and conducts risk assessments before any high-risk processing.

8) UPDATING THE BCRs

Paystack Group will promptly notify Data Protection Authorities of any significant changes affecting its Binding Corporate Rules (BCRs), with the DPO maintaining current BCRs and subsidiary lists. New subsidiaries must be BCR-compliant before data transfers, ensuring continuous regulatory compliance.

9) DATA SUBJECT RIGHTS

As a Group, Paystack's Subsidiaries, employees, agents, contractors, and temporary staff recognize data subjects' rights under data protection laws. We have processes for receiving, resolving (within legal timelines), and communicating decisions on data subject rights requests, addressing appeals and complaints across all our markets. Data subjects have rights including: to be informed about personal data usage; to access personal data held by a controller or processor; to object to all or part of personal data processing, or automated decision-making without human intervention; to correct or delete false/misleading data; and to lodge a complaint with the relevant Supervisory Authority.

Our **Data Subject Rights Request Policy** and **Guidelines for Addressing Data Subject Rights Requests** detail these measures. We maintain documentation of all requests, decisions, and resolution times across all operating markets.

10) DATA BREACH NOTIFICATION

In the event of a personal data breach, the concerned Subsidiary shall report it to the responsible Data Protection Authority in the country of operation, and/or to the concerned data subjects in accordance with the local law. In adhering to the local laws, the Subsidiary shall comply with the local requirements on form, duration, and other legal obligations relating to notification to the Data Protection Authority and the data subjects, where relevant.

The Group and all subsidiaries shall comply with the **Incident Management Framework**.

11) APPLICATION OF DATA PROTECTION PRINCIPLES

To ensure Data Subjects have an equivalent and suitable level of protection, Subsidiaries, employees, agents, individual contractors, and temporary staff agree to apply the legislation of the country with the highest level of Personal Data protection in force in the countries concerned by the Data Transfer, and to comply with our Data Protection Policy and data protection principles. The remedy for violation of this BCR will adhere to the dispute resolution mechanism under applicable contracts.

For contractual obligations, employees shall be treated under the Employment Contract, which is embedded with a data protection clause, and also guided by the **Employee Privacy Notice**. For contractors and agents, they are treated under existing third-party risk management procedures, which include the signing of a Data Processing Agreement, and Due Diligence Procedure.

12) DESCRIPTION OF TECHNICAL AND ORGANISATIONAL MEASURES

Paystack prioritises security through technical and organizational measures across its Subsidiaries. This commitment extends to all employees, agents, individual contractors, and temporary staff, who are obligated through contracts and training to uphold these standards.

A summary of Paystack's technical and organisational measures implemented can be found here.

13) BINDINGNESS AND APPLICABILITY OF BCRs

Paystack Group's Binding Corporate Rules (BCRs) ensure consistent data protection across all subsidiaries, employees, and contractors. Employees can access BCRs internally. Individuals whose data is processed by Paystack Group can request a summary and full details of specific sections (Conflict of BCR over Rules, data protection principles, data subject rights, Guarantees for BCR Implementation, duty to cooperate with supervisory authority, Enforcing the BCRs, Complaints handling procedures). A full copy of the BCRs can be requested by emailing dpo@paystack.com.

If the BCRs are breached, data subjects have enforceable rights, including judicial remedies or complaints to supervisory authorities, specifically for international data transfers, with detailed liability conditions.

Nothing in this BCR shall be construed as overriding data subject rights and interests as prescribed under relevant data protection frameworks such as the Nigeria Data Protection Act, 2023 (as well as subsidiary regulations and guidelines issued by the Nigeria Data Protection Commission), Protection of Personal Information Act, 2013, Kenya's Data Protection Act, 2019 (and subsidiary regulations and guidelines issued by the Office of the Data Protection Commissioner), or DIFC Law No. 5, 2020. Accordingly, anything to the contrary in this BCR, the obligations imposed on a data controller or a data processor in relation to data subject rights and data sovereignty as may be prescribed under or pursuant to the NDP Act, POPIA, DPA, DIFC Law No. 5, and in the processing of data affecting data subjects in Nigeria, South Africa, Kenya, and Dubai International Financial Centre shall remain binding in all circumstances.

14) THIRD PARTY SECURITY RISK MANAGEMENT AUDIT

We manage third-party security and privacy risks by including a supplier audit and inspection obligation in our data processing agreements. We also conduct security and privacy due diligence on third parties using Whistic, a third party risk management tool. Whistic automates periodic due diligence questionnaires for high-risk vendors and stores certifications, whitepapers, and past questionnaires for current and potential vendors.

15) DATA RETENTION AND DELETION PROCEDURE

As a group, we maintain a **Global Data Retention Schedule,** and country-specific data retention schedules to reflect the storage timelines for all the types and categories of personal data processed. In addition, we maintain a Group **Data Retention Policy**, which contains the procedure for permanently deleting data after its expiration.

APPENDICES

The documents referred to in the appendices below are available upon request.

- Appendix 1: Definitions
- Appendix 2: Privacy Policy (separate link)
- Appendix 3: Merchant Privacy Policy (separate link)
- Appendix 4: Data Processing Agreements (separate link)
- Appendix 5: Categories of Data and purposes of Data Transfers and Processing covered by the BCRs
- Appendix 6: List of countries personal data is transferred to

Appendix 1: Definitions

The words and phrases used in the BCRs have the following meanings:

"**Local Data Protection Champion**" means the person in charge within the Group to assure at a local level, that the rules and principles, which are contained in the Employee Handbook and Data Protection Policy ("Policy") and, as may be set forth in more detailed policies and procedures of the Group are properly applied and respected, and to assist Group staff across the world to have a better understanding of these rules and principles;

"**Consent**" means any freely given specific and informed indication of his/her wishes by which the Data Subject signifies his/her agreement to Personal Data relating to him/her being processed;

"**Controller**" (also known as "**Responsible Party**" under other applicable data protection legislation) means the legal person, a Group entity, which alone or jointly with others determines the purposes and means of the Processing of Personal Data;

"**Data Protection Authority**" or "**Supervisory Authority**" means the administrative authority in charge of Personal Data protection in each country in which the Group is present;

"**Data Subject**" means an identified or identifiable natural person to whom the Personal Data that is being processed relates;

"**Group**" means all those companies directly or indirectly controlled by Paystack Inc. (the "**Parent Company**") that are bound by the Policy;

"**Group HQ**" means the group member with the ownership of central administration or decision-making processes, in this case Paystack Payments Limited (HQ, Nigeria).

"**Personal Data**" means any information relating to a natural person who is either identified or identifiable, directly or indirectly, by reference to an identification number or to one or more factor(s) specific to his/her physical, physiological, mental, economic, cultural or social identity;

“Global Data Protection Office”, headed by the Data Protection & Privacy Lead, guarantees that the Policy is properly enforced within the Group, to determine the Policy's general orientation and review any proposed changes. It also handles any infringement to the rules contained in the Policy;

“**Data Protection & Data Privacy Lead**”, means the person running the Global Data Protection Office, in charge within the Group to assure that the Policy, any rules, and procedures of the Group concerning the Personal Data protection are properly applied and respected;

"**Processing**" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

"**Processor**" (also known as “**Operator**” under applicable data protection legislation) means the legal person, whether a Group entity or a Third Party, by which Personal Data is processed on behalf of the Controller;

"**Recipient**" means the natural or legal person, whether a Group entity or a Third Party, to whom/which Personal Data is disclosed;

"**Subsidiary**" means (i) all companies of which Paystack Inc., the Parent Company, either directly or indirectly holds more than half the registered capital and/or (ii) companies which Paystack controls or manages;

"**Third Party**" means any natural or legal person, public authority, agency or any other body than the Data Subject, the Controller, the Processor and the persons who under the direct authority of the Controller or Processor are authorised to process Personal Data;

"Transfer" means any Data disclosure, copy or move via a network, or any Data disclosure, copy or move from one medium to another irrespective of the type of medium, to the extent that such Data is intended for Processing by the Recipient.

Appendix 2 - Privacy Policy

Our country-specific Privacy Policies can be found on our website through this link.

Appendix 3 - Merchant Privacy Policy

Our country-specific Merchant Privacy Policies can be found on our website through this link.

Appendix 4 - Data Processing Agreement

Our country-specific Data Processing Agreements can be found on our website through this link.

Appendix 5 - Categories of Data and purposes of Data Transfers, types of Data Subjects, and Processing covered by the BCRs

Employee data:

The BCRs apply to all Personal Data of the Group's employees that is collected in Nigeria, Ghana, Kenya, South Africa, Dubai, the United Kingdom, United States, Côte d'Ivoire or elsewhere, and is transferred and processed within the Group to manage its human resources at international level as part of its business, such as:

- onboarding data, typically biodata in order to maintain correspondence with employees and fulfil contractual and regulatory obligations;
- organisation, particularly controlling access to the Group's IT systems, technical traceability and administrative workflow monitoring systems, as well as Group Active Directories;
- salary adjustments (annual increases, flexible pay, other pay-related information);
- international mobility;
- human resource development, particularly skills, training and individual and professional development plans; and
- staff administrative management such as travel allowance, expenses, etc.

Personal Data of Group employees that is likely to be transferred includes: first name, last name, contact number, picture, home address, IT identification, professional email address, personal email address, professional location, manager, salaries, sick leave, MAC address, promotion, flexible pay information, type and details of employment contract, individual profile, individual objectives, skills, development requirements, training records, hobbies, mobility and promotion requirements, development plan and any promotion-related information. It may also include lists of work performed, work times and inventory of equipment entrusted to employees. It further includes the names of authors or contributors to documents, as well as the audit trails and electronic signatures needed for compliance with relevant regulations.

Recruitment candidate data:

The BCRs apply to all Personal Data of the Group's recruitment candidate data that is collected in Nigeria, Ghana, Kenya, South Africa, Dubai, United Kingdom, United States, Côte d'Ivoire or elsewhere, that is transferred and processed within the Group to further recruitment activities to drive its business, such as:

- biodata and contact data: name, email address, address, phone number;
- curriculum vitae and any personal information contained therein, including former education institutions, professional certifications etc.;
- background checks;
- references, including referee's name and phone number; and
- interview notes.

Merchant data:

The BCRs apply to all Personal Data of the Group's merchants that is collected in Nigeria, Ghana, Kenya, South Africa, Côte d'Ivoire, or elsewhere, that is transferred and processed within the Group to manage its direct customers at international level as part of its business, such as:

- due diligence, particularly when fulfilling Anti-Money Laundering, Counter-Terror Financing and statutory fraud risk obligations. This type of data specifically includes Know-Your-Customer data such as passport data page, contact details, and proof of address of directors;
- payment information, including bank account details to settle merchants following successful transactions;
- contracts and agreements; and
- transaction data.

Customer data:

The BCRs apply to all Personal Data of Paystack's merchants' customers that is collected in Nigeria, Ghana, Côte d'Ivoire, Kenya, South Africa, or elsewhere, that is transferred and processed within the Group to manage its human resources at international level as part of its business, such as:

- contact data;
- complaints and customer service queries; and
- transaction data.

Vendor data:

The BCRs apply to all Personal Data of the Group's vendors that is collected in Nigeria, Ghana, Côte d'Ivoire, Kenya, South Africa, Dubai or elsewhere, that is transferred and processed within the Group to manage its human resources at an international level as part of its business, such as:

- contact data of contact person;
- contracts and service level agreements;
- security and due diligence questionnaires; and
- payment information, including bank account details to pay vendors for services rendered.

Developer and event attendees' data:

The BCRs apply to all Personal Data of the Group's developers and attendees of events that is collected in Nigeria, Ghana, Dubai, Côte d'Ivoire, Kenya, South Africa, or elsewhere, that is transferred and processed within the Group to manage its human resources at international level as part of its business, such as:

- pictures of attendees;
- engagement of developers within the Paystack community;
- contact data (first name, last name, phone number, work email); and
- job title.

Site visitors' data:

The BCRs apply to all Personal Data of the Group's website visitors that is collected in Nigeria, Ghana, Dubai, Côte d'Ivoire, Kenya, South Africa, Rwanda, Egypt, Dubai, or elsewhere, that is transferred and processed within the Group to manage its human resources at an international level as part of its business, such as:

- location from which they are browsing;
- device ID; and
- browser details.

Appendix 6 - List of Counties Personal Data Is Transferred To

Paystack transfers data within its affiliate companies located in the following countries:

1. Nigeria
2. Kenya
3. Ghana
4. South Africa
5. Côte d'Ivoire
6. Rwanda
7. United Arab Emirates
8. United States of America
9. United Kingdom

Data is stored in Ireland on AWS servers.