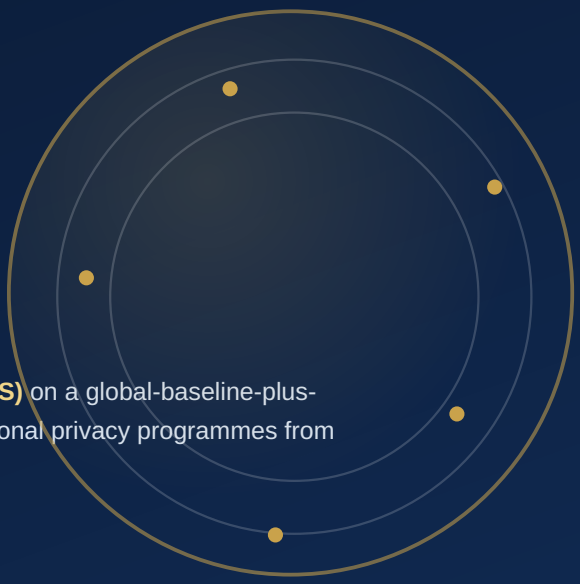
PRIVACY & DATA PROTECTION CONSULTING • PORTFOLIO SAMPLE • 2026

Group GDPR & Privacy Governance Framework



Designing a **Group Privacy Information Management System (PIMS)** on a global-baseline-plus-local-add-ons model — coordinating GDPR, Nigeria's NDPA, and regional privacy programmes from a single source of truth.

Mustafa Alobaidy
Senior GRC & Privacy Consultant
Amazon · Meltwater · Ten Group · 7+ Years GRC & Data Protection

GROUP PIMS
One privacy operating model, many regions

GDPR + NDPA
Multi-jurisdiction control mapping

ROPA & DPIA
Standardised, group-wide workflows

BREACH READY
Legal + Security coordination model

Group GDPR & Privacy Governance Framework

PlayOrbit Group — Representative Consulting Scenario | Prepared by Mustafa Alobaidy, Senior GRC & Privacy Consultant

Table of Contents

> **About this document.** This is a representative consulting scenario built to demonstrate a Group-level privacy governance operating model: a global baseline plus local add-ons, a Group PIMS coordinating regional programmes, standardised RoPA/DPIA workflows, and a multi-jurisdiction control mapping spanning GDPR and Nigeria's NDPA 2023. It is written in the same format as the author's other ISO 27001 / GRC portfolio samples.

SECTION 01

Executive Summary

PlayOrbit Group is a multi-region online sports betting and gaming operator with roughly 3,000 employees across nine operating entities in the UK, the EU, Nigeria, Brazil, and India. Each regional entity built its own privacy programme independently to meet local obligations — GDPR in the UK/EU, the Nigeria Data Protection Act (NDPA) 2023, and LGPD in Brazil. This produced real local compliance, but no group-level visibility: nine different RoPA formats, nine DPIA processes of varying rigour, inconsistent breach-notification timelines, and duplicated evidence collected separately for every audit and regulator request.

This engagement designs a **Group Privacy Information Management System (PIMS)** that sits above the regional programmes without absorbing them: a single global baseline of minimum privacy requirements, with defined local add-ons for jurisdiction-specific obligations, a clear RACI between the Group Privacy Office, Regional DPOs, Legal, and Security, and one evidence library mapped once and reused across every framework and regulator.

9
Regional entities coordinated under one Group PIMS

1 + 9
Global baseline, plus local add-ons per region

2
Core frameworks mapped once — GDPR & NDPA

100%
Target RoPA standardisation across the group

Engagement Objectives

- Define and maintain a single Group privacy baseline — minimum requirements applicable to every operating entity, regardless of local regulation.
- Design the Group PIMS operating model: baseline plus local add-ons, with documented RACI, exception handling, and escalation paths.
- Consolidate nine regionally-owned compliance calendars into one Group view, aligning reporting cadence and evidence standards.
- Standardise RoPA inputs, DPIA workflows, and retention/deletion evidence across all regions.
- Coordinate breach readiness between Legal and Security, with jurisdiction-specific notification paths.
- Build a central evidence library mapped once to the Group control set, reusable across GDPR, NDPA, LGPD, and ISO 27701.

Why this matters commercially. PlayOrbit Group's enterprise payment partners and platform licensors increasingly require evidence of group-wide privacy governance — not just local compliance — before signing or renewing agreements. A coordinated Group PIMS turns nine separate compliance stories into one defensible, auditable narrative.

SECTION 02

Organisational Context & Current State

2.1 Group Profile

Attribute	Details
Organisation	PlayOrbit Group — online sports betting & gaming platform
Headcount	~3,000 employees across 9 operating entities
Regions of operation	United Kingdom, European Union, Nigeria, Brazil, India
Data processed	Player identity & KYC data, payment/transaction data, behavioural & risk data, marketing data
Group functions	Group Privacy Office, Group Security/ISMS, Legal, Procurement
Regional functions	Regional DPO/Compliance Lead, Regional BDM/Programme Manager, local IT & Engineering
Primary regulations	UK GDPR / EU GDPR, Nigeria Data Protection Act (NDPA) 2023, Brazil LGPD, India DPDP Act

2.2 Current State — Fragmented Regional Ownership

Each region currently owns its privacy programme end to end, with no shared template, shared calendar, or shared evidence base. The table below summarises the starting position identified during discovery.

Region	Primary Regulation	Local Owner	RoPA Status	DPIA Process	Maturity
UK	UK GDPR	Regional DPO	Maintained, own format	Ad hoc, legal-led	Developing
EU (multi-country)	EU GDPR	Regional DPO	Partial, per-country variants	Inconsistent across countries	Initial
Nigeria	NDPA 2023	Compliance Lead	Informal register	Not formalised	Ad Hoc
Brazil	LGPD	Compliance Lead	Maintained, own format	Basic screening only	Developing
India	DPDP Act	Local Legal	Not started	Not started	Ad Hoc
Group Level	**None — no group baseline**	**Not assigned**	**No consolidated view**	**No group standard**	**Not Established**

> **Key observation.** Every region is independently solving the same underlying problems — lawful basis documentation, DSAR handling, breach notification, vendor due diligence — using different templates, different terminology, and different evidence formats. None of this work is wasted, but none of it is currently reusable across the Group.

2.3 Compliance Drivers

- **Regulatory exposure:** GDPR fines of up to 4% of global annual turnover; NDPA 2023 introduces comparable penalty exposure with an active enforcement posture from the Nigeria Data Protection Commission.
- **Payments & licensing partners:** acquiring banks and platform licensors increasingly request group-level evidence of data protection governance, not just local certificates.
- **Cross-border data flows:** player and risk data routinely moves between regional entities and group functions (fraud, risk, finance), creating transfer obligations that none of the regional programmes currently document end to end.
- **Operational efficiency:** nine parallel privacy programmes duplicate effort that a shared baseline and evidence library can eliminate.

SECTION 03

Group PIMS Operating Model — Baseline + Local Add-Ons

The operating model is deliberately built to coordinate, not replace, regional ownership. The Group Privacy Office sets and maintains one global baseline of minimum privacy requirements that every entity must meet. Each region then layers jurisdiction-specific "local add-ons" on top — without renegotiating the baseline itself.

3.1 Baseline + Local Add-Ons, Illustrated

Layer	Owner	Examples of Content
Group Baseline	Group Privacy Office	Minimum lawful-basis documentation standard; group RoPA template; group DPIA trigger criteria; minimum retention principles; breach escalation SLA to Group; minimum vendor due-diligence bar.
Local Add-On	Regional DPO / Compliance Lead	UK/EU: ICO/EDPB-specific DSAR timelines and transfer mechanisms. Nigeria: NDPA registration with NDPC, local breach notification to NDPC. Brazil: LGPD-specific ANPD obligations, DPO registration. India: DPDP consent-manager requirements.

3.2 RACI — Group vs Regional Responsibilities

Activity	Group Privacy Office	Regional DPO	Legal	Security
Set group privacy baseline	**A/R**	C	C	I
Maintain local add-ons	C	**A/R**	C	I
RoPA — regional input	I	**A/R**	C	-
RoPA — group consolidation	**A/R**	C	I	-
DPIA execution	C	**A/R**	C	C
DPIA group sign-off (high-risk only)	**A**	R	C	C
Breach detection & triage	I	I	C	**A/R**
Breach legal assessment & notification decision	C	R	**A/R**	C
Vendor privacy due diligence	C	R	C	C
Evidence library maintenance	**A/R**	R	I	C
Regulatory change tracking	**A**	R	R	I

A = Accountable, R = Responsible, C = Consulted, I = Informed.

3.3 Exception Handling & Escalation

- **Local deviation request:** a region may request a documented exception to a baseline requirement where local law conflicts or local practice is not yet feasible. Submitted to the Group Privacy Office with business and legal justification.
- **Time-bound approval:** exceptions are approved for a fixed period (typically 6 months) with a remediation date, logged in the Group risk register, and reviewed at the next Group governance cycle.
- **Escalation path:** unresolved exceptions, overdue DPIAs, or breach notification disagreements escalate from Regional DPO → Group Privacy Office → Group Risk & Compliance Committee → Executive Sponsor.

SECTION 04

Multi-Jurisdiction Mapping — GDPR & Nigeria NDPA

To avoid re-deriving privacy controls for every new jurisdiction, the Group baseline is built once against GDPR (the most prescriptive regime PlayOrbit Group is subject to) and then cross-mapped to each additional regulation. The mapping below illustrates the approach for Nigeria's NDPA 2023, the jurisdiction explicitly in scope for this engagement alongside GDPR. The same method extends to LGPD (Brazil) and the DPDP Act (India).

Dimension	GDPR (UK/EU)	Nigeria NDPA 2023	Group Baseline Control
Regulator	ICO (UK) / national DPAs (EU)	Nigeria Data Protection Commission (NDPC)	Single regulator contact register per entity, held centrally
Lawful basis for processing	Six lawful bases under Art. 6	Equivalent lawful-basis grounds under the Act	Group lawful-basis decision log, one format, mapped per region
DPO appointment	Mandatory for large-scale/high-risk processing	Mandatory for controllers/processors of "major importance"	Group DPO appointment policy; named Regional DPO per entity
RoPA / processing register	Required under Art. 30	Equivalent record-keeping expectation under the Act	One Group RoPA template — see Section 5
DPIA trigger	Required for high-risk processing (Art. 35)	Required for high-risk processing under the Act	One Group DPIA screening tool — see Section 6
Breach notification to regulator	Without undue delay, and in any case within 72 hours where feasible	Notification obligation to the NDPC; timelines confirmed with local counsel per filing	One Group breach SLA with regional notification annex — see Section 7
Cross-border transfer	Adequacy decisions, SCCs, or equivalent safeguards	Transfer restrictions with permitted-mechanism requirements under the Act	Group transfer-mechanism register, reviewed per corridor
Data subject / data principal rights	Access, rectification, erasure, restriction, portability, objection	Comparable rights framework under the Act	One Group DSAR intake & fulfilment process

Note on scope. This mapping is built for portfolio/training purposes to demonstrate methodology. Specific deadlines, thresholds, and registration obligations under NDPA 2023 (and any other local regulation) must always be validated against the current statutory text and confirmed with qualified local counsel before being relied on operationally — this is precisely the role the Group Privacy Office plays in coordination with Legal in each region.

SECTION 05

Group RoPA Standard

The single biggest blocker to a group-wide privacy view was the absence of a common RoPA format. Each region collected broadly the same information, but in different spreadsheets, different terminology, and different levels of detail — making it impossible to answer a simple group-level question ("where does PlayOrbit Group process biometric KYC data, and under what lawful basis?") without manually reconciling nine documents.

5.1 Standard RoPA Fields

Field	Purpose	Owner
Processing Activity Name	Plain-language description of the activity (e.g. "Player KYC verification")	Regional DPO
Purpose of Processing	Why the data is processed; ties to lawful basis	Regional DPO
Lawful Basis	One of the group-standard lawful basis categories	Regional DPO / Legal
Data Categories	Including flag for special-category / sensitive data	Regional DPO
Data Subjects	Players, employees, vendors, etc.	Regional DPO
Recipients / Sharing	Internal teams, processors, group functions, regulators	Regional DPO
Cross-Border Transfer	Destination, mechanism, and safeguard reference	Regional DPO / Legal
Retention Period	Linked to the Group retention schedule (Section 7)	Regional DPO / Records Owner
Security Measures	Reference to applicable ISMS controls — reused, not re-described	Security
DPIA Status	Required / not required / completed, with link to DPIA record	Regional DPO
Group Risk Reference	Link to the relevant entry in the Group risk register	Group Privacy Office

5.2 RoPA Workflow

5.3 Current vs Target State

Metric	Current	Target (6 months)
Regions with a maintained RoPA	4 of 9 (informal)	9 of 9 (group template)
RoPA formats in use	4 different formats	1 group template
Group-level visibility	None	Single consolidated register, refreshed quarterly
Special-category data flagged	Inconsistent	100% flagged with lawful basis recorded

SECTION 06

Group DPIA Workflow

DPIAs were previously triggered inconsistently — sometimes by Legal, sometimes by Engineering, sometimes not at all. The Group standard introduces a single screening tool used everywhere, with a clear threshold for when a full DPIA is required and when Group sign-off is mandatory.

6.1 Screening Triggers — Full DPIA Required If:

- The activity involves large-scale processing of special-category data (e.g. biometric KYC, health data referenced in responsible-gambling checks).
- The activity involves systematic monitoring or profiling used to make decisions with legal or similarly significant effect on a player (e.g. automated risk/affordability scoring).
- The activity introduces a new cross-border transfer corridor not already covered by an approved mechanism.
- The activity introduces a new third-party processor with access to player identity or payment data.
- A regional regulator (e.g. NDPC) or Group Privacy Office designates the activity as high-risk.

6.2 Workflow Steps

6.3 DPIA RACI

Step	Regional DPO	Group Privacy Office	Legal	Security
Screening	A/R	I	-	-
Full DPIA drafting	A/R	C	C	C
Risk treatment plan	R	C	C	A
Group sign-off (high-risk)	R	A	C	C
Filing into evidence library	R	A/R	I	I

SECTION 07

Retention, Deletion & Breach Readiness

7.1 Group Retention & Deletion Evidence Standard

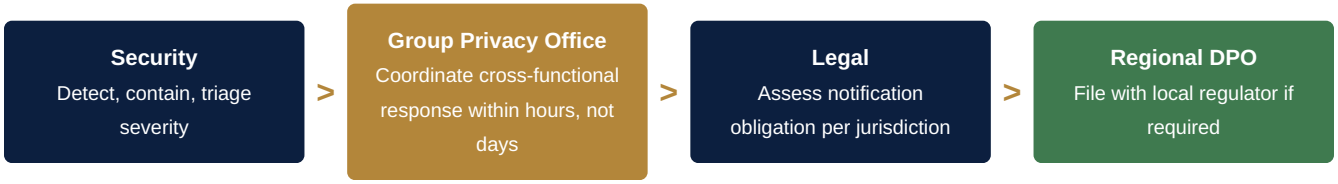
Retention periods already exist informally in most regions, but evidence that deletion actually happened is largely missing. The Group standard requires every RoPA entry to link to a retention rule and to a defined evidence type proving deletion or anonymisation occurred.

Data Category	Illustrative Retention Driver	Deletion / Anonymisation Method	Evidence Type
Player KYC / identity documents	AML & licensing record-keeping obligations	Secure deletion post retention window	Deletion job log + sign-off
Transaction & payment data	Financial/tax record-keeping obligations	Archival then secure deletion	Archive manifest + deletion certificate
Marketing consent & preference data	Group marketing policy	Deletion on consent withdrawal or inactivity	Consent platform export log
Responsible-gambling / risk indicators	Regulatory & safeguarding obligations	Anonymisation post case closure	Anonymisation script output + reviewer sign-off
Employee HR data	Local employment law	Secure deletion post offboarding window	HRIS deletion confirmation

Retention periods are jurisdiction-specific and must be confirmed per region with Legal; the table above illustrates the evidence-standard methodology rather than stating fixed durations.

7.2 Breach Readiness — Coordination Model

Breach response currently sits mostly with Security at a technical level, with Legal engaged late and Regional DPOs sometimes not engaged at all. The Group model makes the handoff explicit and time-bound.



Stage	Target Internal SLA	Owner
Detection to Security triage	Within hours of detection	Security
Security triage to Group Privacy Office notification	Same business day	Security
Legal notification-obligation assessment	Within 24 hours of escalation	Legal + Regional DPO
Regulator notification (where required)	Per applicable statutory deadline for each jurisdiction	Regional DPO
Post-incident evidence filed to Group library	Within 5 business days of closure	Group Privacy Office

> **Note on timelines.** Statutory notification deadlines (e.g. GDPR's 72-hour regulator notification standard) differ by jurisdiction and must be confirmed against current law with Legal at the time of an incident. The internal SLAs above are designed to leave enough runway to meet the tightest applicable external deadline, whichever jurisdiction is involved.

SECTION 08

Central Evidence Library & Third-Party Privacy Artifacts

8.1 Map Once, Reuse Everywhere

The same underlying control evidence is currently produced multiple times — once per framework, once per region, once per audit. The Group evidence library inverts this: each control is evidenced once, then mapped to every framework that requires it.

Group Control	GDPR	NDPA 2023	ISO 27701	Internal Audit
Lawful basis register / RoPA	Art. 30	Record-keeping requirement	Clause 6.4 / Annex B	Quarterly RoPA check
DPIA records	Art. 35	High-risk processing requirement	Clause 6.5	Sampled per audit cycle
DSAR fulfilment log	Art. 12–22	Data subject rights provisions	Clause 7.3	Timeliness sampled monthly
Breach register & notifications	Art. 33–34	Breach notification provisions	Clause 6.13	Reviewed at every incident close
Vendor due-diligence pack	Art. 28	Processor obligations	Clause 7.2	Annual vendor tier review
Retention & deletion logs	Art. 5(1)(e)	Storage-limitation principle	Clause 7.4	Sampled per audit cycle

8.2 Standardised Third-Party Privacy Artifacts

Procurement and Legal currently run vendor due diligence per region, using whatever questionnaire that region created. The Group standard introduces one tiered approach.

Vendor Tier	Trigger	Required Artifact	Review Cadence
Tier 1 — Critical	Processes player identity, KYC, or payment data	Full privacy & security questionnaire, DPA/SCCs, evidence of certifications	Annual
Tier 2 — Significant	Processes other personal data (e.g. marketing, support tooling)	Standard questionnaire, DPA	Every 18 months
Tier 3 — Limited	No personal data access, or minimal/anonymised data	Lightweight self-attestation	On contract renewal

- Questionnaires, minimum security/privacy requirements, and evidence packages are owned jointly by the Group Privacy Office, Legal, and Procurement, and reused for every region rather than redrafted locally.
- Vendor evidence is filed into the same central library, mapped to the relevant Group control — avoiding a second parallel "vendor compliance" archive.

SECTION 09

12-Month Implementation Roadmap

Phase 1 — Foundation (Months 1–3)

Initiative	Deliverable	Owner
Group Privacy Baseline	Approved baseline policy + local add-on template	Group Privacy Office
Group Governance	RACI, escalation path, and exception-handling process signed off	Group Privacy Office / Legal
Consolidated Compliance Calendar	Nine regional calendars merged into one Group view	Group Privacy Office
RoPA Template Rollout	Group RoPA template issued to all nine regions	Regional DPOs

Phase 2 — Standardisation (Months 4–7)

Initiative	Deliverable	Owner
RoPA Consolidation	9 of 9 regions reporting into the central RoPA repository	Group Privacy Office
DPIA Standardisation	Group DPIA screening tool live in every region	Regional DPOs / Group Privacy Office
Multi-Jurisdiction Mapping	GDPR & NDPA mapping complete; LGPD & DPDP mapping underway	Legal / Group Privacy Office
Breach Coordination Model	Joint Legal–Security breach playbook tested via tabletop exercise	Legal / Security

Phase 3 — Evidence & Vendor Standardisation (Months 8–10)

Initiative	Deliverable	Owner
Central Evidence Library	Controls mapped once across GDPR, NDPA, ISO 27701	Group Privacy Office
Retention & Deletion Evidence	Deletion evidence standard live for top 5 data categories	Security / Records Owners
Vendor Tiering	Tier 1 vendors reassessed under the new questionnaire	Procurement / Legal

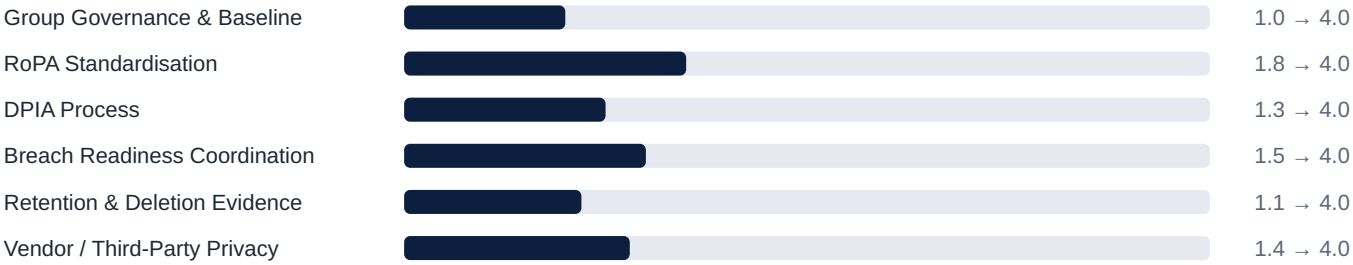
Phase 4 — Continuous Monitoring (Months 11–12)

Initiative	Deliverable	Owner
Group Risk Register Review	First full quarterly review with all regions reporting	Group Privacy Office
Regulatory Change Tracking	Process live for tracking GDPR/NDPA/LGPD/DPDP changes into the baseline	Legal / Group Privacy Office
Management Review	First Group-level privacy governance review presented to leadership	Group Privacy Office

SECTION 10

Maturity Scorecard & Closing Recommendations

10.1 Group Privacy Maturity — Current vs Target



Scale: 1 = Ad Hoc, 2 = Developing, 3 = Defined, 4 = Managed. Bars show current maturity; target is Managed (4.0) within 12 months.

10.2 Strategic Recommendations

- **Name a Group Privacy Office owner first.** Without a single accountable owner, the baseline will drift back into nine separate programmes within a year.
- **Start with RoPA, not policy.** A working, group-wide RoPA gives immediate visibility and is the foundation every other workstream (DPIA, breach, evidence library) depends on.
- **Make the baseline genuinely minimal.** Over-specifying the global baseline invites local non-compliance; reserve detail for the local add-ons regions actually need.
- **Joint-own breach readiness with Security from day one.** Privacy and security incident response cannot run as separate processes when most breaches are technical in origin.
- **Reuse evidence aggressively.** Every control evidenced once and mapped to GDPR, NDPA, LGPD, DPDP, and ISO 27701 reduces audit burden across every region simultaneously.

10.3 Conclusion

A Group PIMS does not ask PlayOrbit Group's regions to give up local ownership of their privacy programmes — it gives them a shared baseline, a shared template, and a shared evidence library so that local compliance work counts at the group level too. Within 12 months, PlayOrbit Group moves from nine disconnected privacy programmes to one coordinated, auditable, multi-jurisdiction privacy governance model — built on the same baseline-plus-local-add-ons logic that scales as the Group enters new markets.

> **Prepared by Mustafa Alobaidy** — Senior GRC & Privacy Consultant. Experience spans GDPR-aligned governance frameworks for high-confidentiality, multi-region client environments (Ten Group), executive compliance reporting for sensitive international stakeholders (Meltwater), and GDPR-aligned risk assessment across EMEA operations (Amazon). This document is a representative consulting scenario prepared to demonstrate methodology and is not associated with any real organisation named "PlayOrbit Group."