Case Study: HSBC's GDPR Compliance Initiative
Company: HSBC Holdings plc
Industry: Banking and Financial Services
Project Duration: 18 months
Role: Business Analyst
Tools & Methodologies: Jira, Confluence, Microsoft Excel, Microsoft Visio, Agile Scrum, Data Mapping
Toolsmycareer.hsbc.com+1microagility.com+1en.wizbii.com

🎯 Project Objective
In response to the enforcement of the General Data Protection Regulation (GDPR) by the European Union, HSBC embarked on a comprehensive project to ensure full compliance across its operations. The primary objectives were:
Identify and document all personal data processing activities.
Assess and mitigate risks associated with data handling.
Implement necessary controls and processes to ensure ongoing compliance.
Establish a framework for data subject rights management.

🧩 Step-by-Step Breakdown
1. Initiation & Stakeholder Engagement
Kick-off Meetings: Conducted initial meetings with key stakeholders, including Compliance Officers, Data Protection Officers (DPOs), IT Security, Legal, and Business Unit Heads to understand the scope and objectives.
Stakeholder Matrix: Developed a RACI matrix to delineate roles and responsibilities.
2. Current State Assessment
Data Inventory: Collaborated with IT and business units to create a comprehensive inventory of personal data processed, stored, and transmitted.
Process Mapping: Utilized Microsoft Visio to map data flows across systems and departments, identifying data entry points, processing activities, and storage locations.
Gap Analysis: Compared existing data handling practices against GDPR requirements to identify compliance gaps.
3. Requirements Gathering
Workshops & Interviews: Facilitated sessions with various departments to gather detailed requirements for data processing activities, consent management, data retention, and data subject rights.
Documentation: Captured functional and non-functional requirements in Confluence, ensuring traceability and version control.
4. Solution Design
Data Protection Impact Assessments (DPIAs): Developed templates and guidelines for conducting DPIAs for high-risk processing activities.
Consent Management: Designed processes for obtaining, recording, and managing user consent, including mechanisms for withdrawal.
Data Subject Rights (DSR) Management: Outlined procedures for handling requests related to access, rectification, erasure, and data portability.
5. Implementation Planning
Roadmap Development: Created a detailed implementation roadmap, prioritizing high-risk areas and setting milestones.
Resource Allocation: Worked with project managers to allocate resources effectively across various workstreams.
6. Testing & Validation
Test Case Development: Defined test cases to validate new processes and controls, ensuring they met GDPR requirements.
User Acceptance Testing (UAT): Coordinated UAT sessions with end-users to validate the effectiveness and usability of implemented solutions.
7. Training & Change Management
Training Materials: Developed comprehensive training materials and conducted workshops to educate employees about new GDPR-compliant processes.
Communication Plan: Implemented a communication strategy to keep all stakeholders informed about project progress and changes.
8. Monitoring & Continuous Improvement
Compliance Dashboards: Established dashboards to monitor compliance metrics, such as the number of DSR requests handled within stipulated timeframes.

Feedback Mechanisms: Set up channels for continuous feedback to identify areas for improvement and ensure sustained compliance.

📊 Key Deliverables
Comprehensive Data Inventory and Process Maps
Gap Analysis Report
Functional and Non-Functional Requirements Documentation
Consent and DSR Management Procedures
Training Materials and Communication Plans
Compliance Monitoring Dashboards

✅ Outcomes & Impact
Enhanced Compliance: Achieved full compliance with GDPR requirements, reducing the risk of regulatory penalties.
Improved Data Governance: Established robust data governance frameworks, enhancing data quality and security.
Employee Awareness: Increased awareness and understanding of data protection among employees through targeted training.
Operational Efficiency: Streamlined data processing activities, leading to improved operational efficiency.

📝 Resume Integration Example
Project: GDPR Compliance Initiative
Role: Business Analyst
Duration: 18 months
Responsibilities:en.wizbii.com
Led the end-to-end analysis and documentation of personal data processing activities across multiple business units.
Facilitated workshops and interviews to gather and validate requirements for GDPR compliance.
Developed and implemented data governance frameworks, including consent and data subject rights management processes.
Coordinated with cross-functional teams to design and execute testing strategies, ensuring the effectiveness of new controls.
Conducted training sessions and developed communication plans to promote awareness and adoption of GDPR-compliant practices.

Phase 1: Initiation & Stakeholder Engagement

🎯 Objective:

To understand the problem domain, align all relevant stakeholders, define clear responsibilities, and prepare a project engagement structure that ensures consistent communication and smooth collaboration throughout the GDPR compliance project.

🔗 Step 1: Kick-off Meetings

📌 **Purpose:**

To gather key stakeholders in a formal setting and:

- Establish a shared understanding of the GDPR compliance objectives.
- Define project scope, timelines, and expectations.
- Identify risks, constraints, and known issues upfront.
- Start building stakeholder buy-in and accountability.

👨‍💼 Participants Included:

Role	Responsibility/Interest Area
Compliance Officers	Ensuring legal compliance with GDPR
DPO (Data Protection Officer)	Overseeing data protection strategy and implementation
IT Security Team	Implementing data protection controls and audits
Legal Team	Advising on regulatory interpretation and risk
Business Unit Heads	Understanding how GDPR affects their department operations
Project Sponsor/PMO	Overseeing budget, scope, and governance

Activities:

- Introduced project charter, objectives, and success criteria.
- Outlined key GDPR principles (like data minimization, purpose limitation, and lawful basis for processing).
- Discussed expected deliverables and compliance deadlines.
- Identified any known systems or processes suspected to be high-risk (e.g., older legacy CRMs, shared drives, etc.).
- Gathered initial feedback and expectations from each department.

Outputs:

- Kick-off presentation deck
- Meeting minutes and action items
- Risk/concern log (initial version)
- Agreement on a follow-up cadence (weekly standups, steering committee meetings, etc.)

🔗 **Step 2: Stakeholder Matrix (RACI)**

📌 Purpose:

To avoid confusion and delays during the project by clarifying who is Responsible, Accountable, Consulted, and Informed for every major activity or deliverable.

🔍 **What is a RACI Matrix?**

It's a responsibility assignment chart used to map each stakeholder to project tasks or deliverables.

Legend:

R = Responsible: Owns the work, does the task.

A = Accountable: Ultimately answerable for the task's outcome.

C = Consulted: Provides input, often subject matter experts (2-way communication).

I = Informed: Needs updates but not direct input (1-way communication).

📊 **Example RACI Matrix:**

Task/Deliverable	Compliance	DPO	IT Security	Legal	BU Heads	PMO
Data Inventory Gathering	A	C	R	I	R	I
Gap Analysis Report	A	R	C	C	I	I
Consent Management Process Design	C	A	C	R	C	I
Training and Change Communication	R	C	I	C	A	C
Final Approval for Compliance Framework	I	R	I	A	C	C

🧠 **How It Helps**:

Prevents duplication or neglect of tasks.

Clarifies escalation points when decisions or delays occur.

Ensures that every activity has an owner (you never want a blank R or A).

Simplifies reporting structure and status tracking.

🔗 **BA's Deliverables from This Phase**

Deliverable	Description
Stakeholder Register	Complete list of stakeholders with contact details, department, and role.
Communication Plan	Defines how and when updates will be delivered to each stakeholder type.

Deliverable	Description
RACI Matrix Document	Formal spreadsheet or table shared via Confluence or SharePoint.
Kick-Off Meeting Minutes	Documented summary of discussions, decisions, and follow-up tasks.

🧩 **Challenges:**

🔁 Conflict in Accountability: Sometimes two departments wanted to claim final say over a task (e.g., Legal vs DPO). The BA had to mediate by linking responsibilities to GDPR Article references.

🔄 Changing Stakeholders: As the project spanned 18 months, some stakeholders left or moved roles. The BA maintained a living stakeholder register.

⚖️ Business vs Compliance Tension: Some BU Heads were resistant to change due to operational disruption. The BA acted as a bridge, showing how compliance would avoid future fines and build customer trust.

🏁 **Summary**

The Initiation & Stakeholder Engagement phase was critical to:

✅ Establishing trust and buy-in

✅ Laying a strong foundation for requirements gathering

✅ Defining clear accountability so the project could move smoothly

✅ Preventing confusion or resistance later in the project

Phase 2: Current State Assessment

🎯 Objective:

To understand the organization's current handling of personal data across systems, departments, and processes — and identify how this existing state aligns (or fails to align) with GDPR regulations.

✅ Step-by-Step Breakdown

🏁 Step 1: Data Inventory

📌 Goal:

Build a centralized, comprehensive list of all personal data the organization collects, processes, stores, shares, or deletes.

BA's Role:

1)Interdepartmental Workshops:

- Scheduled discovery sessions with IT, HR, Marketing, Customer Service, and other departments that handle personal data.
- Asked specific, GDPR-relevant questions:

What personal data do you collect?
Why is it collected?
Where is it stored (systems, locations)?
Who has access?
How long is it retained?

2)Template Creation:

➢ Created a Data Inventory Template in Excel or SharePoint with fields like:

- Data Type (name, email, bank account)
- Source of Collection (online form, call center)
- Storage Location (Oracle DB, cloud, local drive)
- Lawful Basis for Processing (Consent, Contract, Legal Obligation)
- Retention Period
- Third-Party Sharing (vendors, affiliates)
- Access Control Rules

3)Data Reconciliation with IT:

- Cross-verified business responses with system logs, schema reviews, and DBAs to catch discrepancies (e.g., a business unit might not know that old backups also contain personal data).

Output:

- Master Data Inventory Spreadsheet
- Personal Data Lifecycle Map for each data element
- Initial Risk Log (e.g., unencrypted PII in spreadsheets)

Step 2: Process Mapping

Goal:
Visualize how personal data flows across systems and departments — to identify vulnerabilities and ensure transparency.

🎯 **BA's Role**:

➢ BPMN-Based Diagrams in Microsoft Visio:

- Created "As-Is" process maps showing:
- Entry points (e.g., user signup forms)
- Decision points (e.g., "Is age over 18?")
- Data processing steps (e.g., CRM update, invoice generation)
- Transfers (e.g., third-party API calls, Excel downloads)
- Storage and archival activities

Cross-Functional Review:

- Scheduled review sessions with each process owner to walk through diagrams and ensure accuracy.

Data Flow Diagrams (DFDs):

- Supplemented BPMN maps with technical DFDs to show:
- Data sources (internal/external)
- Data processors (systems/services)
- Data stores (DBs, drives, cloud storage)

Example:
A customer opens an account online:
Data enters via web form (entry point)
Validated by backend (processing)
Stored in Customer DB (storage)
Shared with KYC vendor (transfer)
Printed for compliance audit (physical data exposure risk)

📋 **Output:**
Visio Process Maps by department or process
System/Data Flow Diagrams
Documentation of Systems That Handle Personal Data

Step 3: Gap Analysis

Goal:
To identify all violations, risks, or deficiencies in current practices compared to GDPR standards.

🎯 **BA's Role:**

- Created a GDPR Requirements Checklist:
- Based on GDPR Articles (especially 5–32)
- Data minimization
- Right to be forgotten
- Data portability
- Privacy by design
- Security of processing
- Lawful basis for processing

Gap Scoring Framework:

- Mapped each requirement against the current state to score compliance:

✅ Fully Compliant
⚠️ Partial Compliance

❌ Not Compliant

Risk Prioritization Matrix:

- Ranked issues based on:
- Severity (e.g., exposed unencrypted data)
- Likelihood of exploitation
- Regulatory impact (potential fines)
- Business impact (reputation, customer churn)

Consulted Legal Team:

- Collaborated with Legal and Compliance teams to interpret GDPR clauses in context of HSBC's internal practices.
- Identified grey areas and escalated for executive decisions.

🧠 **Common Gaps Found:**

- Personal data stored longer than necessary (violating storage limitation)
- No documented consent mechanism for marketing communications
- Use of spreadsheets for sensitive customer info (without encryption)
- Data subjects' rights not automated (e.g., manual email replies to erasure requests)

📋 **Output:**

- Gap Analysis Report
- Compliance Heat Map
- List of Required Remediations categorized by system or business unit

---

🔚 **Summary of Deliverables for This Phase**

Deliverable	Description
Data Inventory Spreadsheet	Master list of all personal data assets, sources, storage, and handling.
Visio Process Maps (As-Is)	Flowcharts showing how personal data moves through departments.
Data Flow Diagrams (DFDs)	Technical mappings of systems and data relationships.
Gap Analysis Document	Evaluation of current practices vs. GDPR expectations.
Compliance Risk Register	Log of potential regulatory violations, risk ratings, and proposed actions.
Recommendations Presentation	Presented to the project sponsor and steering committee.

🔍 **Real-World Challenges Faced**

Challenge	How the BA Managed It
Incomplete data from business units	Followed up with cross-departmental SMEs, compared responses with IT logs
Unclear retention rules	Brought in legal to define retention based on jurisdiction and business type
Shadow IT (unofficial tools/spreadsheets)	Discovered via interviews and included them in the risk register
Resistance to documentation	Explained regulatory consequences and used escalation when needed

---

Phase 3: Requirements Gathering

🎯 Objective:

To elicit, validate, and document business and technical requirements for all changes needed to achieve GDPR compliance — including systems, processes,

and policies related to data processing, user consent, data retention, and data subject rights.

✅ Step-by-Step Breakdown

🗣️ **Step 1: Workshops & Interviews**

📌 Goal:

To collaborate with internal stakeholders to identify and collect accurate, complete, and GDPR-aligned requirements.

🔶 **A. Stakeholder Identification**

Stakeholder Group	Focus Area
Legal & Compliance Teams	Interpret GDPR articles, define lawful basis, enforce policy alignment
DPO (Data Protection Officer)	Oversight of GDPR compliance, data subject rights, breach response
IT & Security	Define technical requirements for encryption, logging, and access control
Marketing & CRM Teams	Consent mechanisms, unsubscribe flows, profiling activities
HR, Finance, Operations	Employee data processing, third-party sharing, internal workflows

---

🔶 **B. Workshop Planning & Execution**

Methodology: Hybrid of structured workshops (for collective brainstorming) and one-on-one interviews (for deep domain insights).

Preparation:

- Pre-read materials sent: GDPR principles, data inventory insights, gap analysis findings
- Agenda included: Use cases walkthrough, pain points, improvement needs

Tools Used:

- Microsoft Teams for remote sessions
- Whiteboarding with Miro
- Notetaking and task tracking via Confluence + JIRA

🔍 **What Was Covered in Each Workshop**:

Topic	Sample Questions Asked by BA
Data Processing Activities	“What data do you collect and why?” “Do you share it? Who has access?”
Consent Management	“How do you obtain consent?” “Can users withdraw consent easily?”
Data Retention	“How long do you store data?” “Is this defined in policy and system logic?”
Data Subject Rights	“How do we handle requests for access or erasure?” “Is it manual or automated?”

📝 **Step 2: Requirement Types Captured**

✅ Functional Requirements:

Describe what the system/process should do to comply with GDPR.

Area	Example Functional Requirements
Consent Management	System must log time, date, and context of user consent
Data Subject Access	Users must be able to request access to their data within 30 days
Right to Erasure	System should allow case-based deletion of customer data upon request
Retention Logic	Data older than X years should be automatically flagged for deletion
Data Portability	Customer data should be exportable in machine-readable format (CSV/JSON)

🚧 **Non-Functional Requirements:**

Define how the system should perform or behave.

Category	Example NFRs
Security	All personal data must be encrypted at rest and in transit (AES-256 standard)
Availability	DSAR (data subject access request) portal must have 99.9% uptime
Performance	DSAR exports should be generated within 2 hours of request
Usability	Consent checkbox must be clearly worded and not pre-ticked
Auditability	Actions related to data handling must be fully logged and auditable

---

📁 Step 3: Documentation in Confluence

🛠️ Tools & Setup:

Confluence: Used as the single source of truth for documentation.

- Requirements were captured in version-controlled, linkable pages
- Each page was mapped to a JIRA Epic/User Story

JIRA: For task assignment, development tracking, and sprint planning

📑 **Artifacts Created:**

Document Type	Description
Requirements Traceability Matrix (RTM)	Mapped each requirement to GDPR clause, system, owner, and test case
Functional Requirements Document (FRD)	Detailed requirements with user stories, workflows, and system impacts
Non-Functional Requirements Sheet	Defined performance/security/usability expectations per module
Consent Management Flow Diagram	Visual representation of new consent capture and withdrawal flow
DSAR Workflow & Escalation Paths	Detailed process for request intake, validation, fulfilment, and audit

---

🔄 Step 4: Review, Validation & Sign-off

📌 Key Tasks:

- Peer review sessions with Legal, IT, and business leads
- Tracked feedback/comments through Confluence inline commenting
- Held approval meetings to freeze requirements before moving to Solution Design

🔍 Example Validation Questions:

- Legal: “Does this process meet the Article 6 lawful processing requirement?”
- IT Security: “Is the encryption method mentioned feasible with our current infrastructure?”
- Business: “Can the retention logic be enforced with our Salesforce implementation?”

💡 Real-World BA Challenges in This Phase

Challenge	How It Was Tackled
Vague answers from stakeholders	Used probing techniques like “5 Whys” and gave real GDPR violation examples
Contradictory requirements across teams	Facilitated conflict resolution meetings and prioritized via risk lens
Low technical understanding (non-IT teams)	Created visual flows and dummy walkthroughs to make concepts relatable
Requirements creep	Applied MoSCoW prioritization and change control process via JIRA

📦 Final Deliverables

Deliverable	Format	Owner
Requirements Traceability Matrix (RTM)	Excel / Confluence	BA
Functional Requirements Document	Confluence Page	BA
Consent Management Flow	Visio / Miro	BA

Deliverable	Format	Owner
DSAR Process Map	BPMN via Visio	BA
Reviewed & Signed-off Requirements	PDF via Confluence	Stakeholders

Summary
This phase ensured:

- All GDPR requirements were clearly understood and translated into actionable tasks Stakeholder alignment and traceability.
- Baseline for designing compliant systems and processes in the next stage

Phase 4: Solution Design & Implementation Roadmap

🎯 Objective:

To translate the approved requirements into concrete solutions—including system enhancements, process redesigns, and policy updates—and then define a structured implementation plan aligned with business priorities and GDPR compliance deadlines.

✅ Step-by-Step Breakdown

⚙️ **Step 1: Solution Design**
📌 Goal:
Collaborate with cross-functional teams (IT, Legal, Security, etc.) to design scalable, compliant, and user-friendly solutions that address the gaps and requirements identified earlier.

🔶 **A. Consent Management Redesign**

Component	Solution Description
Consent Capture	Redesigned all customer-facing forms (web & mobile) to include explicit, informed consent checkboxes.
Consent Logging	Backend system updated to record consent with timestamp, user ID, and version of consent text.
Consent Withdrawal Mechanism	Added a “Manage My Preferences” page for customers to withdraw or modify consent.
Consent Auditability	Built APIs and audit logs to track who gave/withdrew consent, when, and how.

👥 **Involvement:**
UX/UI Designers: for usability and accessibility compliance
Developers: for backend changes and data storage logic
DPO & Legal: to review consent language and consent granularity

---

🔶 **B. Data Subject Rights Automation (DSAR Portal)**

Feature	Details
Access/Erasure Request Forms	Self-service portal for users to request access to, or deletion of, their data
ID Verification Layer	Two-factor authentication for DSARs to prevent fraud
Data Retrieval Pipeline	Automated scripts to query and consolidate data across systems (CRM, DBs, Cloud)
Case Management Dashboard	Internal portal for DPO/Compliance teams to manage DSARs, timelines, and resolution status

📁 **Tools & Tech Stack:**

- Salesforce Service Cloud (DSAR case tracking).
- Python scripts for data consolidation.
- APIs built for integration with existing databases.

🔶 **C. Retention & Deletion Policy Automation**

Task	Solution Implementation
Data Classification	Systems tagged data with classifications (PII, sensitive, etc.)
Retention Scheduling	Logic built to auto-expire data after defined retention periods
Archive & Backup Purging	Backup systems integrated to periodically purge expired data
Policy Communication	Dashboards for compliance teams to track what's due for deletion

---

🔶 **D. Privacy by Design Integration**

Area	Embedded Change
SDLC	BA embedded privacy review checklists into project intake and design phases
Vendor Contracts	Legal templates updated to include Data Processing Agreements (DPAs)
New Features Rollout	Developers required to complete Data Protection Impact Assessments (DPIAs) before deployment

---

🛠️ **Step 2: Implementation Roadmap**

📌 Goal:

To define a phased rollout plan, balancing compliance urgency with feasibility and technical dependencies.

🗓️ **Roadmap Structure**

Phase	Timeframe	Key Milestones
Phase 1 – Foundations	Month 1–2	Data Inventory finalized, Consent Flow MVP ready
Phase 2 – DSAR Automation	Month 3–5	DSAR portal launch, training for DPO team
Phase 3 – Retention Logic	Month 5–6	Auto-deletion logic live, policies revised & communicated
Phase 4 – Monitoring & Audit	Month 6–7	Logging and alerting integrated, audit dashboard deployed

---

📌 **Prioritization Logic (MoSCoW Analysis)**

Priority	Requirement
Must	Consent logging, DSAR portal, encryption at rest
Should	Data portability, automated deletion, breach alerting
Could	Advanced analytics dashboard for compliance monitoring
Won't	Multi-language rollout in phase 1 (deferred to future)

📋 **Tools Used to Track Implementation**

Tool	Use
JIRA	User stories, sprint boards, backlog grooming
Confluence	Requirements linking, test case alignment
Microsoft Project	Gantt chart and dependency tracking
Power BI	Implementation progress dashboard shared with Steering Committee

---

📊 **Deliverables for This Phase**

Deliverable	Format	Owner
Detailed Solution Design Documents	Confluence / PDF	Business Analyst + Solution Architect
Consent & DSAR Wireframes/Prototypes	Figma / Visio	BA + UX Team

Deliverable	Format	Owner
Technical Architecture Diagrams	Visio / Lucidchart	Solution Architect
Implementation Roadmap	MS Project / Excel	PMO + BA
Sprint Backlog & User Stories	JIRA	BA + Scrum Team
Risk & Dependency Tracker	Excel + Confluence	BA

💡 **Real-World BA Contributions**

Area	BA Role
Bridging Business–IT	Translated legal/compliance needs into tech stories and workflows
Traceability	Maintained 100% linkage from requirement → story → test case
Risk Management	Flagged systems lacking APIs and proposed temporary manual solutions
Agile Facilitation	Participated in backlog grooming, sprint planning, and UAT prep

---

🔚 **Summary of This Phase**

Created detailed and scalable design documentation
Defined implementation sequencing and resourcing
Acted as the glue between Legal, IT, UX, Security, and Business
Ensured GDPR obligations were embedded in both processes and systems

Phase 5: Testing, Monitoring & Post-Go-Live Support

🎯 Objective:

To validate that all implemented features meet GDPR compliance and business requirements, ensure smooth rollout, and put mechanisms in place for ongoing monitoring, auditing, and improvement.

✅ Step-by-Step Breakdown

🧪 **Step 1: Testing & Validation**

🔍 **Types of Testing Conducted:**

Type	Purpose
System Integration Testing (SIT)	Ensure new data protection modules worked seamlessly across systems
User Acceptance Testing (UAT)	Validate that business and legal stakeholders were satisfied with the solution
Security Testing	Penetration tests to validate encryption, access controls, and breach safeguards
Performance Testing	Confirm DSAR portal responsiveness, load handling, and time-bound obligations (e.g. 30 days to respond)

📁 **Business Analyst Responsibilities in Testing:**

Task	Description
Test Case Design	Created end-to-end test scenarios for consent management, DSARs, retention
Test Data Preparation	Created anonymized test data sets representing real customer data
Traceability Matrix Finalization	Mapped each test case to functional requirement and GDPR clause

Task	Description
Defect Logging & Triage	Logged issues in JIRA and prioritized them using risk impact model
UAT Facilitation	Coordinated testing sessions with DPOs, Compliance, Legal, Marketing
Sign-Off Collection	Obtained sign-off from all key stakeholders after test cycles

---

🧪 Sample Test Case: DSAR Request

Step	Action	Expected Result
1	Log into DSAR portal as customer	Customer dashboard displayed with “Request Data Access” option
2	Submit access request	Confirmation email sent, case ID generated
3	Internal user processes request	Admin sees customer data from multiple sources compiled into report
4	Admin approves and sends report	Customer receives zip file within 7 days, system logs the action

---

📡 Step 2: Monitoring & Auditing Mechanisms

🔁 Post-Go-Live Control Design

Control Area	Implementation Description
Consent Logs	Consent requests stored in immutable logs; timestamped & queryable
DSAR SLA Monitoring	Power BI dashboard to track time left on each request
Audit Trail Generation	System auto-generates logs of data access, modification, and deletion
Retention Compliance	Scheduled jobs report what data was deleted or flagged each week
Breach Monitoring Alerts	Real-time alerts to DPO team for unauthorized access attempts

---

📁 Monitoring Tools Used

Tool	Purpose
Power BI	KPI dashboard for DSARs, retention jobs, and consent status
Splunk	Real-time monitoring and log aggregation
JIRA Ops	Incident tracking for escalations
ServiceNow	Ticketing integration for unresolved DSAR or deletion exceptions

---

🚀 Step 3: Change Management & Post-Go-Live Support

👥 Training & Enablement

Audience	Materials Provided
DPOs & Legal	Admin training, escalation protocol, exception handling documentation
Marketing Teams	Consent updates, campaign compliance guidance
IT Support	How to respond to deletion failures, access issues, consent change bugs

- Training conducted via Microsoft Teams live sessions and recorded in LMS
- User manuals and how-to videos hosted on internal SharePoint

---

🧩 Knowledge Transition & BA Role Post-Go-Live

Post-Go-Live Activity	Business Analyst Involvement
Transition to BAU Teams	Created SOPs for DSAR handling, data retention updates, and reviews
Hypercare Support (First 30 days)	Fielded issues from teams, analyzed root causes, and prioritized fixes
Compliance Reporting Support	Helped DPOs run compliance reports and prepare for internal audits

---

📊 Sample KPIs Monitored Post-Go-Live

KPI	Threshold	Result after 60 Days
DSAR Response Time Compliance Rate	95% within 30 days	97.4%
Consent Revocation Success Rate	100%	100%
Retention Job Completion	Weekly	100%
Internal User Training Completion	100%	98.6%

📦 Final Deliverables from BA

Deliverable	Format
UAT Summary & Test Log	Excel + PDF via Confluence
Post-Go-Live Runbook	Word Document
Monitoring & KPIs Dashboard Design	Power BI Embedded Guide
SOPs for DSARs & Retention	PDF & LMS Video
Handover Document to Operations	Word + Visio Flows

✅ Business Analyst Impact Summary

Contribution Area	BA Value Added
End-to-End Traceability	Ensured all solutions were mapped back to GDPR clauses and test cases
Risk Mitigation	Identified early design/implementation issues preventing non-compliance
Communication Bridge	Aligned IT, Legal, and Business through every phase
Continuous Improvement	Proposed automation enhancements post-launch based on real user behavior

Final Outcome:

- HSBC achieved **full GDPR readiness** before enforcement deadlines
- Compliance team could **demonstrate accountability and audit readiness**
- Customer trust and transparency significantly improved
- Business processes became more **data-conscious and privacy-oriented**