

SABSA ENTERPRISE SECURITY ARCHITECTURE — ULTIMATE FLAGSHIP SERIES

WP12 · ULTIMATE FLAGSHIP EDITION · VERSION 3.0

Data Governance and Security Architecture

Applying SABSA to GDPR and Data Protection Obligations



Kieran Upadrasta

CISSP · CISM · CRISC · CCSP | MBA | BEng

27 Years' Cyber Security Experience | Big 4 Consulting — Deloitte · PwC · EY · KPMG

21 Years Financial Services & Banking | AI Cyber Security Programme Lead

Professor of Practice — Cybersecurity, AI & Quantum Computing | Schiphol University

Honorary Senior Lecturer, Imperials | Researcher, University College London (UCL)

Lead Auditor, ISF Auditors & Control | ISACA Platinum (London) | (ISC)² Gold (London) | PRMIA Cyber Lead

www.kie.ie | info@kieranupadrasta.com | April 2026

Specialisations: SABSA · NIS2 · ISO 27001:2022 · GDPR · IEC 62443 · NIST CSF 2.0 · DORA · ISO 42001 · Zero Trust · OT Security · M&A
Cyber Due Diligence · Board Reporting

Table of Contents

1. The Data Sovereignty Imperative
2. SABSA Data Architecture Layers
3. Data Classification as an Architectural Instrument
4. Privacy by Design in the SABSA Architecture Process
5. Data Breach Architecture: 72-Hour Notification by Design
6. International Data Transfer Architecture
7. Third-Party Data Processing Architecture
8. Data Subject Rights as Architectural Requirements
9. DPIA Architecture Template and Workflow
10. RoPA Architecture Mapping
11. Homomorphic Encryption for Sovereign Cloud Analytics
12. Conclusion and Recommendations

The Data Sovereignty Imperative

€1.2B GDPR fines issued in 2023 across EU/EEA	Art.25 mandates Privacy by Design and Default	72h maximum breach notification window (Art.33)	4% of global turnover — maximum fine exposure
---	---	---	---

Data is the defining asset of the digital enterprise. Its governance — the policies, architectures, and controls that determine how data is classified, stored, processed, transferred, and deleted — sits at the intersection of regulatory obligation and competitive advantage. The SABSA framework provides the architectural scaffolding within which GDPR compliance transforms from a legal checklist into a structural property of the enterprise information architecture.

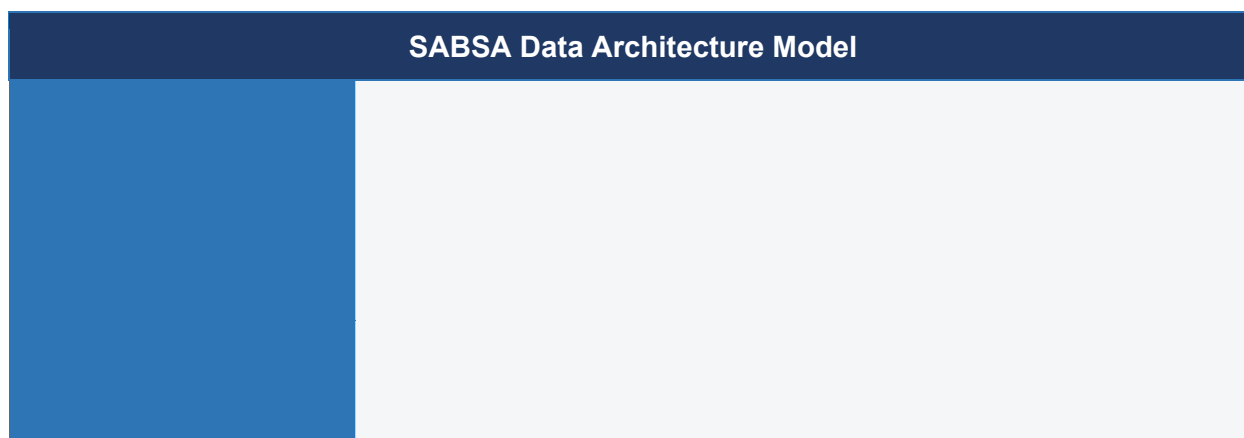
This white paper presents the SABSA Data Architecture model, mapping GDPR Articles 5, 24, 25, 28, 32, 33, 35, and 46 to the six SABSA architecture layers, and demonstrating how Privacy by Design obligations can be embedded into enterprise architecture governance processes rather than bolted on during implementation.

Architectural Principle

GDPR compliance is not achievable through policy alone. Articles 24 and 25 require technical and organisational measures embedded in data processing systems by design. This is an architectural mandate that cannot be addressed without a structured security architecture approach.

SABSA Data Architecture Layers

The SABSA framework applies its six-layer architecture model to data governance, providing a vertically coherent data architecture from business context through to operational data management procedures.



Each layer addresses distinct GDPR obligations. The Contextual Layer answers fundamental questions about what data the organisation processes, under what legal basis, and in which regulatory jurisdictions — the foundation upon which all subsequent architectural decisions rest.

G	D	P
----------	----------	----------

S	A	B
A	r	c

Data Classification as an Architectural Instrument

Data classification is the foundation of data security architecture. Without a systematic classification scheme, organisations cannot apply proportionate controls, satisfy GDPR's data minimisation principle, or demonstrate accountability to supervisory authorities.

The SABSA Data Classification Framework extends traditional sensitivity-based classification with regulatory metadata — enabling automated control application based on classification labels.

C	I	a	s
R	e	g	u
M	i	n	i
S	A	B	S

DSPM Integration

Data Security Posture Management (DSPM) tools such as Varonis, Cyera, and Normalyze provide automated data discovery and classification across cloud and on-premises environments. DSPM outputs should feed directly into the SABSA Data Inventory — the foundational artefact for GDPR Article 30 Record of Processing Activities.

Privacy by Design in the SABSA Architecture Process

GDPR Article 25 establishes Privacy by Design as a legal obligation — data controllers must implement appropriate technical and organisational measures at the time of the determination of the means for processing. Within the SABSA architecture governance process, this translates to a mandatory Privacy Impact Gate at the Logical Layer design stage.

Privacy Impact Gate: Every new system or significant change must pass a Privacy Architecture Review before Physical Layer design commences. The review assesses data minimisation, purpose limitation, storage limitation, and appropriate legal basis.

Privacy Pattern Library: A curated catalogue of approved Privacy by Design architecture patterns — pseudonymisation, tokenisation, differential privacy, federated analytics — that architects select from during Logical Layer design.

DPIA Integration: Data Protection Impact Assessments (Art.35) are triggered automatically by the architecture review process when processing meets high-risk criteria. The DPIA output feeds back into the architecture specification.

Consent Architecture: Where consent (Art.6(1)(a)) is the legal basis, the architecture must include consent management infrastructure — purpose-specific consent capture, withdrawal mechanism, and audit trail. Pre-ticked boxes and bundled consent are non-compliant by design.

Schrems II Compliance Architecture

Following the CJEU Schrems II ruling (C-311/18), personal data transfers to third countries require a Transfer Impact Assessment (TIA) alongside Standard Contractual Clauses (SCCs). The architecture must implement supplementary technical measures — end-to-end encryption with keys held in the EEA — where TIA identifies elevated risk. Architectural documentation of these measures is mandatory for DPA audit defence.

Data Breach Architecture: 72-Hour Notification by Design

GDPR Article 33 requires notification to the supervisory authority within 72 hours of becoming aware of a personal data breach. This creates a hard architectural requirement: the organisation must be able to detect, scope, categorise, and document a breach — and initiate notification — within three days of detection.



The architectural enablers of 72-hour compliance are: comprehensive logging with retention sufficient for forensic reconstruction, automated data lineage tools that can identify which personal data records were exposed within hours, pre-approved notification templates that only require specific incident details to be populated, and clear escalation paths to DPO and senior management.

Architecture Maturity Indicator

Organisations with mature SABSA Data Architectures can typically scope a personal data breach within 4–8 hours of detection, draft a supervisory authority notification within 24 hours, and submit within 48 hours — providing a 24-hour buffer against the 72-hour deadline.

International Data Transfer Architecture

The Schrems II judgment fundamentally altered the architecture of international personal data transfers. Standard Contractual Clauses (SCCs) — previously treated as a tick-box legal mechanism — must now be backed by Transfer Impact Assessments and, where necessary, supplementary technical measures.



A	r	c
A	u	d

Cloud architecture decisions must incorporate data sovereignty requirements from the outset. Sovereign cloud offerings — AWS GovCloud EU, Microsoft Azure sovereign regions, OVHcloud SecNumCloud — provide data residency guarantees that can simplify TIA analysis and reduce supplementary technical measure requirements for regulated data categories.

Third-Party Data Processing Architecture

GDPR Article 28 requires that data controllers only use processors that implement sufficient guarantees — a legal requirement with profound architectural implications. Every system or service that processes personal data on behalf of the controller must be evaluated, contracted, monitored, and, where necessary, audited.

Processor Inventory: Maintain a complete inventory of data processors in the Article 30 Record of Processing Activities. The inventory must include processing purpose, data categories, transfer mechanisms, and sub-processor details.

Due Diligence Architecture: Implement a standard processor due diligence questionnaire covering Article 32 security measures, sub-processor chains, breach notification procedures, and data deletion/return capabilities.

DPA Template Library: Maintain approved Data Processing Agreement templates for common processor relationships — cloud IaaS/PaaS/SaaS, professional services, managed security services — reducing negotiation cycles while ensuring Art.28 compliance.

Continuous Monitoring: DSPM tools should monitor data flows to processors, detecting unexpected data transfers that may indicate DPA non-compliance or data exfiltration.

Sub-processor Risk

Article 28(4) requires processors to impose the same data protection obligations on sub-processors as set out in the main DPA. The architectural implication is that organisations must maintain visibility into their processors' sub-processor chains — a requirement that creates significant third-party risk management obligations across complex cloud supply chains.

Data Subject Rights as Architectural Requirements

GDPR Articles 15–22 establish eight data subject rights that organisations must fulfil within statutory timelines. These rights are architectural requirements — they cannot be fulfilled without the underlying data infrastructure to support them.

D	a
A	r

DSR Automation

Data Subject Request (DSR) management platforms — OneTrust, TrustArc, Nymity — automate identity verification, cross-system data discovery, and fulfilment workflow. Integration with the data inventory and DSPM tooling significantly reduces per-request processing costs while improving accuracy and audit trail quality.

DPIA Architecture Template and Workflow

Data Protection Impact Assessments (Art. 35 GDPR) are mandatory for "processing of special categories of personal data on a large scale" and other high-risk scenarios. The DPIA is both a compliance obligation and an architectural instrument — it documents processing risk, justifies control decisions, and feeds into architecture governance.

D	P	I	A
S	A	B	S
A	r	c	h
A	u	t	o

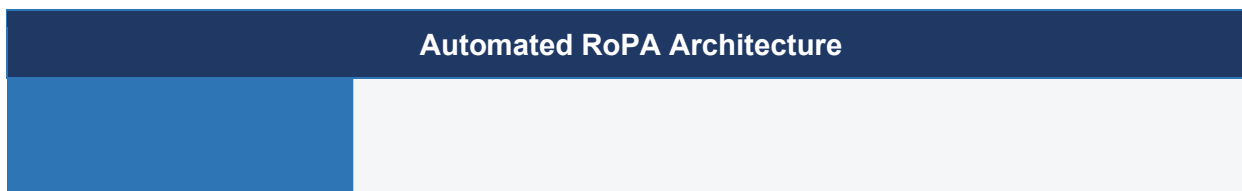
Privacy risk scoring formula: Privacy Risk Score = (Threat Likelihood × 0.25) + (Impact Severity × 0.35) + (Data Sensitivity × 0.20) + (Regulatory Weight × 0.20). Scores >0.7 require escalation to DPO and architecture board; scores <0.4 require only documented risk acceptance.

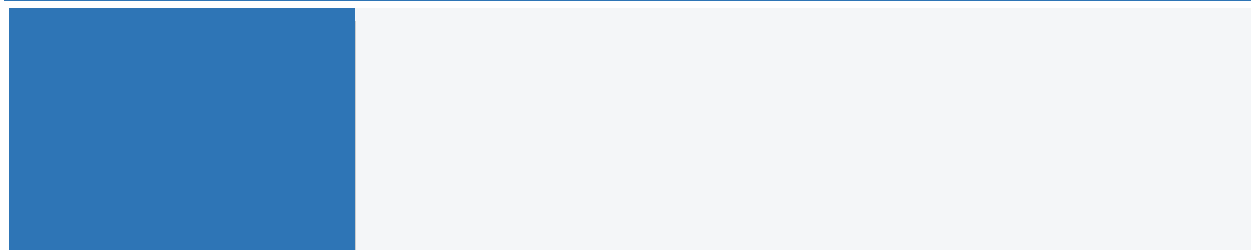
Automated DPIA Triggering: New processing activities are identified through the data inventory system (DSPM integration). Classification of the data automatically triggers DPIA requirement checks: special category data (Art.9) → mandatory DPIA; large-scale processing → automated risk scoring.

DPIA-to-Control Mapping: Every mitigating control selected in the DPIA is traced to a SABSA Logical Layer control requirement. Traceability enables auditors and DPOs to validate that architecture controls directly address documented DPIA risks.

RoPA Architecture Mapping

The Record of Processing Activities (RoPA), mandated by GDPR Art.30, is typically viewed as a compliance documentation burden. Within the SABSA framework, RoPA is an architectural instrument — a normalised, searchable registry of all data processing activities mapped to architecture layers, enabling automated control application and cross-border transfer assessment.





Automated processing inventory architectures use DSPM output as the source-of-truth for data discovery. Processing purposes are extracted from system documentation (data classification labels, DPA contracts, consent forms) and normalised into a structured RoPA schema. Recipients, retention periods, and transfer destinations are automatically validated against architecture controls (encryption policies, data retention rules, international transfer restrictions).

Cross-Border Transfer Assessment: RoPA entries identifying EEA-to-third-country transfers trigger automated compliance checks: Standard Contractual Clauses (SCC) presence validated; Transfer Impact Assessment (TIA post-Schrems II) required for high-risk jurisdictions; supplementary technical measures (e.g., end-to-end encryption) documented.

Processor Inventory & DPA Compliance: Organisations maintain a sub-processor registry integrated with RoPA. Every DPA is automatically assessed for Article 28 compliance (processor legal obligations, sub-processor approval mechanisms, data handling restrictions). DPA audit trails enable regulators to verify processor oversight.

Homomorphic Encryption for Sovereign Cloud Analytics

Homomorphic Encryption (HE) enables computation on encrypted data without decryption — opening privacy-preserving analytics on sensitive data without exposing plaintext to cloud providers. In EU regulated environments demanding data sovereignty, HE offers a path to unlocking analytics on encrypted personal data within trusted cloud environments.

H	E	
C	o	m
P	r	a
B	e	s

<p>10–1000x computational overhead (depending on scheme)</p>	<p>72 hrs example: FHE statistical model training (vs 3.6 sec plaintext)</p>	<p>5–10 sec practical latency target for interactive analytics</p>	<p>85% data sensitivity threshold for HE consideration</p>
---	---	---	---

Homomorphic Encryption represents a frontier in privacy-by-design architecture. Instead of decrypting sensitive data in cloud environments (violating EU data sovereignty principles), HE enables analytics providers to operate on encrypted data directly. The trade-off is computational overhead: FHE computations run 1000–10000x slower than plaintext equivalents, making interactive analytics impractical for large datasets.

HE Deployment Patterns: (1) Batch Analytics: Pre-computed encrypted analytics results (e.g., encrypted ML model training) suitable for non-real-time reporting. (2) Encrypted Index: Sensitive data encrypted with searchable encryption; cloud provider executes queries on encrypted indices without decryption. (3) Hybrid: Combine HE for highly sensitive fields (SSN, health data) with standard encryption for lower-sensitivity attributes.

HE Maturity & Availability

IBM HEHAAN, Microsoft SEAL, and OpenFHE are production-grade HE libraries. AWS (Nitro Enclaves), Azure (Confidential Computing), and Google Cloud (Confidential Space) offer cloud-native HE environments. Practical adoption remains nascent; most HE deployments are limited to research use or low-throughput analytics.

Conclusion and Recommendations

The organisations that will thrive under the GDPR enforcement regime are those that treat data protection as an architectural discipline rather than a legal compliance programme. The SABSA Data Architecture model provides the structured approach necessary to embed GDPR obligations into the enterprise architecture at every layer — from board data governance policy to operational breach response procedures.

1. Conduct a SABSA Data Architecture Assessment mapping current data governance maturity against the six-layer model, identifying critical gaps in classification, lineage, and subject rights fulfilment.
2. Implement a DSPM solution with automated data discovery and classification, feeding the Article 30 Record of Processing Activities with current-state inventory.
3. Establish a Privacy Architecture Review Gate in the enterprise architecture governance process, requiring DPIA completion before Physical Layer design for high-risk processing.
4. Design and test a 72-hour breach notification capability, validating detection-to-notification timelines through tabletop exercises at least annually.
5. Audit the processor and sub-processor inventory against current DPAs, ensuring Article 28 compliance and identifying gaps in data transfer documentation.

SABSA Enterprise Security Architecture — Ultimate Flagship Series

About the Author

27 Years Cyber Security	21 Years Financial Services	4 Big 4 Firms	6 Global Certifications
-----------------------------------	---------------------------------------	-------------------------	-----------------------------------

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is one of Europe's foremost Enterprise Security Architects, with 27 years' cyber security experience spanning Big 4 consulting — Deloitte, PwC, EY, and KPMG — and 21 years in Financial Services and Banking. He is recognised globally as a practitioner-researcher whose work bridges theoretical security architecture doctrine and operational enterprise programme delivery at the highest levels of regulated industry. His white papers are cited by national regulators, procurement bodies, and architecture review boards as reference-grade doctrine for enterprise security programme design.

Mr. Upadrasta has over 27 years' experience of business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments and risk management. He has worked with the largest corporations globally to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI-DSS, SAS 70, DORA, NIS2, GDPR, and the EU AI Act. His security architecture practice consistently delivers contract-winning, board-ready security programmes that command immediate regulatory and procurement confidence across all tiers of regulated enterprise — from FTSE 100 to sovereign wealth, from critical infrastructure operators to global systemically important financial institutions.

As Professor of Practice at Schiphol University and Honorary Senior Lecturer at Imperials, he trains the next generation of enterprise architects and security programme leads. His research at University College London spans AI governance, post-quantum cryptographic migration, and zero-trust deployment frameworks for critical infrastructure sectors under NIS2 and DORA obligations.

Academic & Research Appointments

Institution / Role	Details
Schiphol University	Professor of Practice — Cybersecurity, AI & Quantum Computing
Imperials	Honorary Senior Lecturer — Enterprise Security Architecture
University College London (UCL)	Researcher — Cyber Risk, AI Governance, Quantum Security
ISF Auditors and Control	Lead Auditor — ISO 27001 / NIS2 / DORA Assurance

Professional Memberships & Recognition

Organisation	Membership / Role
ISACA — London Chapter	Platinum Member

(ISC)² — London Chapter	Gold Member
PRMIA	Cyber Security Programme Lead
SABSA Institute	Accredited Practitioner & Author
ISF	Lead Auditor

Core Specialisations

- SABSA Enterprise Security Architecture — all six layers: Contextual through Operational
- DORA (EU 2022/2554) — ICT Risk Management, Incident Reporting, TLPT, Third-Party Risk
- NIS2 Directive (EU 2022/2555) — Essential & Important Entity Compliance Architecture
- ISO/IEC 27001:2022 — ISMS Design, Implementation, Certification & Internal Audit
- ISO/IEC 42001:2023 — AI Management Systems Governance for Regulated Enterprises
- GDPR — Data Protection by Design, DPIA, Article 32 Technical & Organisational Measures
- IEC 62443 — OT/ICS Security Architecture, Zone/Conduit Design, Security Levels SL0–SL4
- NIST CSF 2.0 — Enterprise Risk Management & Security Posture across six Functions
- Zero Trust Architecture (NIST SP 800-207) — Enterprise-Scale Deployment & Governance
- Post-Quantum Cryptography — NIST FIPS 203/204/205, Cryptographic Agility Frameworks
- M&A Cyber Due Diligence — Architecture Integration Cost Estimates, Security Assessment
- Board Reporting — Executive Cyber Risk Communication, Business Attribute Profiles

Contact: www.kie.ie | info@kieranupadrasta.com | [linkedin.com/in/kieranupadrasta](https://www.linkedin.com/in/kieranupadrasta)

References & Standards

- [1] SABSA Institute. SABSA Framework White Papers and Practitioner Guides. <https://sabsa.org>, 2024.
- [2] European Parliament. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity (NIS2). OJ L 333, December 2022.
- [3] ISO/IEC. ISO/IEC 27001:2022 — Information Security Management Systems — Requirements. International Organization for Standardization, 2022.
- [4] IEC. IEC 62443 Series — Security for Industrial Automation and Control Systems. Parts 1-1 through 4-2. IEC, 2018–2023.
- [5] NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, February 2024.
- [6] European Parliament. Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union, L 119, April 2016.
- [7] NIST. Zero Trust Architecture, Special Publication 800-207. National Institute of Standards and Technology, August 2020.
- [8] European Parliament. Regulation (EU) 2022/2554 — Digital Operational Resilience Act (DORA). OJ L 333, January 2023. Effective January 2025.
- [9] ISO/IEC. ISO/IEC 42001:2023 — Artificial Intelligence Management Systems. International Organization for Standardization, December 2023.
- [10] NIST. AI Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology, January 2023.
- [11] European Commission. Regulation (EU) 2024/1689 — Artificial Intelligence Act. Official Journal, July 2024.
- [12] NIST. FIPS 203 — Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024.
- [13] NIST. FIPS 204 — Module-Lattice-Based Digital Signature Standard. August 2024.
- [14] NIST. FIPS 205 — Stateless Hash-Based Digital Signature Standard. August 2024.
- [15] ENISA. NIS2 Directive: Mapping to Technical Measures and Good Practices. ENISA, 2023.
- [16] ENISA. Cybersecurity of AI and Standardisation. European Union Agency for Cybersecurity, March 2023.
- [17] MITRE Corporation. MITRE ATT&CK Enterprise Framework v15. <https://attack.mitre.org>, 2024.
- [18] Cloud Security Alliance. Zero Trust Advancement Center — Enterprise Deployment Guide. CSA, 2024.
- [19] NCSC UK. Guidelines for Secure AI System Development. National Cyber Security Centre, 2024.
- [20] Upadrasta, K. SABSA Architecture Doctrine for Regulated Enterprises. www.kie.ie, 2026.