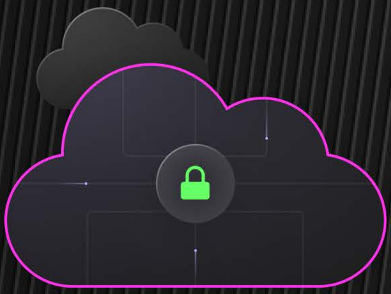
sentra



GDPR Compliance Guide: How to Operationalize GDPR Data Protection Controls with Sentra

Table of Contents

Introduction

On paper, GDPR is clear. In practice, it collides with sprawling cloud, SaaS, and on-prem environments, where many organizations struggle to say with confidence what data they have or where it lives.

Sentra is a cloud-native data security platform built to close that gap by combining:

- **Data Security Posture Management (DSPM)**
  Continuous discovery, classification, and risk analysis for data across IaaS, PaaS, SaaS, and on-prem environments.
- **Data Detection & Response (DDR)**
  Monitoring data access and movement to detect anomalous behavior and potential exfiltration.
- **Data Access Governance (DAG)**
  Mapping identities to data and enforcing least-privilege access.
- **AI-aware coverage**
  Protecting training data and AI agents/coplots while aligning with frameworks such as GDPR, EU AI Act, NIST AI RMF, and ISO/IEC 42001.

Sentra's AI-powered classification delivers over 95% accuracy across structured, semi-structured, and unstructured data, automatically detecting PII, PHI, PCI, secrets, and proprietary business data at petabyte scale. All scanning runs inside your own environment, so sensitive payloads never leave your control.

GDPR Principles (Article 5) & Lawfulness (Articles 6–9)

GDPR Control / Principle	How Sentra Helps
Lawfulness, Fairness, Transparency (Art. 5(1)(a), 6–9)	Sentra discovers and classifies personal data (including PII/PHI/PCI) across cloud data platforms, databases, data lakes, and SaaS apps, providing an accurate map of where regulated data lives and how it is used. This inventory underpins lawful-basis analysis and transparency documentation by showing which systems process personal data, for what business purposes, and in which regions.
Purpose Limitation (Art. 5(1)(b))	By classifying data with **business context** (e.g., HR, finance, healthcare) and tracking which workloads and AI pipelines consume it, Sentra helps you detect when data is being repurposed beyond its original purpose, such as production customer data copied into experimental AI training buckets. Findings can feed into DPIAs and internal approvals before expanding processing purposes.
Data Minimization (Art. 5(1)(c))	Sentra's Data Risk Assessments highlight **stale, unused, and duplicate data sets** containing personal data—including shadow copies in S3, snapshots, and non-production environments. This makes it practical to remove or consolidate unnecessary copies of personal data and enforce "collect and keep only what you need" at scale.
Accuracy (Art. 5(1)(d))	While Sentra does not correct data, it identifies fragmented and duplicated stores of personal data across systems (data lakes, warehouses, SaaS apps), giving data owners the visibility needed to unify records and avoid inconsistent or outdated copies. This supports operational data quality processes overseen by privacy and data governance teams.

GDPR Control / Principle	How Sentra Helps
Storage Limitation (Art. 5(1)(e))	Sentra surfaces regulated data stores that contain sensitive information but lack proper retention controls. It identifies large volumes of personal data in legacy or long-unused locations—such as old snapshots, exports, and test environments—and classifies them by sensitivity and business purpose. This enables you to tie retention policies and automated deletion workflows to real data assets, not just theoretical records.
Integrity & Confidentiality (Art. 5(1)(f), see also Art. 32)	Through DSPM, DAG, and DDR, Sentra continuously evaluates whether personal data is properly encrypted, restricted to appropriate identities, and shielded from public or external exposure. It detects misconfigurations (e.g., public buckets with PII), over-permissive access (identities with broad rights to sensitive stores), and suspicious activity on those assets.
Accountability (Art. 5(2))	Sentra maintains **audit-ready evidence** of where personal data resides, who can access it, how it is protected (encryption, access controls, residency), and what issues and remediations have occurred over time. This provides the factual basis for demonstrating accountability to supervisory authorities, auditors, and internal risk committees.

Data Subject Rights & Transparency (Articles 12–23)

GDPR Control / Right	How Sentra Helps
Transparent Information, Communication (Art. 12–14)	Sentra's classification and context (data type, data subject region, business system) allow privacy teams to inventory the actual systems that hold personal data, so notices and privacy documentation reflect reality rather than assumptions. This supports accurate privacy notices, records of processing, and transparency about where and how personal data is used—including in AI systems.
Right of Access (Art. 15)	By discovering and classifying personal data across cloud and SaaS environments—including shadow and non-production repositories—Sentra gives privacy teams a **comprehensive map** of where a data subject's information may reside. Sentra automates the handling of DSAR requests by accurately discovering and classifying personal data across all environments and providing compliance teams the ability to generate DSAR reports, trigger data deletion requests, and verify removal of data—all from a single interface or using te Sentra API. With accurate PII mapping, Sentra reduces response time, ensures compliance, and increases customer trust.
Right to Rectification (Art. 16)	Sentra highlights **duplicate and inconsistent stores** of personal data (e.g., multiple exports or backups that still contain PII), enabling teams to target which systems must be updated after rectification requests so that old versions do not silently persist.

GDPR Control / Principle	How Sentra Helps
Right to Erasure (Art. 17)	Using Sentra’s DSAR capabilities, governance teams can quickly locate a data subject’s records across systems, trigger removal workflows, and then verify that erasure has been applied completely.
Right to Restriction (Art. 18) & Objection (Art. 21)	By mapping identities to data and highlighting which systems use personal data for analytics or AI, Sentra enables security and privacy teams to enforce restrictions (e.g., pausing access to certain stores or AI workloads for particular classes of data) while requests are under evaluation.
Right to Data Portability (Art. 20)	Sentra shows where a data subject’s personal data is stored (and in what formats), making it easier to design automated exports and standardized schemas for portability responses. Its built-in DSAR acceleration feature can generate subject-centric views for direct export and also feed existing DSAR or privacy portals with accurate scope.
Rights related to Automated Decision-Making & Profiling (Art. 22)	Organizations need clear visibility into which datasets feed automated decision-making and profiling. Sentra identifies datasets containing personal data that could be used in profiling contexts, and classifies them as higher-risk for governance purposes, enabling organizations to demonstrate to auditors what types of data are collected, their sensitivity and region, and how they are used in connection with automated decision workflows.

Security of Processing (Article 32) & Breach Notification (Articles 33–34)

GDPR Control / Obligation	How Sentra Helps
Appropriate Technical & Organizational Measures (Art. 32(1))	Sentra continuously assesses the **security posture** of data stores containing personal data including **encryption status (at rest and in transit), masking and tokenization coverage, access logging, and backup/snapshot usage,** as well as encryption status, network exposure, access controls, use of snapshots, and AI/analytics linkages. It highlights high-risk combinations such as public S3 buckets with PII, external identities with access to regulated datasets, or AI workloads trained on restricted data.
Confidentiality, Integrity, Availability, and Resilience (Art. 32(1)(b–d))	Through DSPM and DAG, Sentra provides continuous visibility into access permissions and data exposure, helping organizations enforce least-privilege access by identifying over-permissive roles, external sharing, configuration drift, and employee access to sensitive personal data that could undermine confidentiality and integrity. DDR adds behavioral monitoring to detect suspicious reading, copying, or exfiltration of personal data that may indicate credential theft, insider threat, or ransomware staging supporting reduced insider risk and faster response.
Regular Testing and Evaluation of Measures (Art. 32(1)(d))	Sentra's continuous posture checks, risk scoring, and compliance dashboards effectively **re-test your data controls on every scan,** surfacing new misconfigurations or risks as your environment changes. Evidence can be exported for internal audits and security certifications.

GDPR Control / Obligation	How Sentra Helps
Breach Detection and Investigation (Arts. 33–34)	When anomalous activity is detected (such as large data exports, new access by AI workloads, or access from unusual identities or region) Sentra's DDR correlates the activity with continuous data classification in real time to identify the compromised data and initiate an incident. This provides incident response teams with rapid, evidence-based impact visibility, supporting timely and well-documented notification. In addition Sentra's up to date data catalog and activity feed enables organizations to conduct deep investigations and generate requiered incident reports demonstrating pre-incident controls, incident scope, and post-incident remediation to regulators.

Data Transfers & Cross-Border Controls (Articles 44–49)

GDPR Control / Obligation	How Sentra Helps
Lawful International Transfers (Arts. 44–46)	Sentra classifies data with region and residency context, and provides out-of-the-box policies such as quickly identifying when EU data appears in locations or accounts that fall outside your approved transfer mechanisms (e.g., SCCs, intra-group agreements). Sentra's reports then provide the evidence base for transfer impact assessments and for demonstrating that appropriate technical safeguards (encryption, restricted access, logging) are in place to support lawful international transfers.

GDPR Control / Obligation	How Sentra Helps
Transfer Impact Assessments & Contractual Safeguards (Arts. 46–49)	By mapping **which data, in which regions, is accessed by which identities and services** (including AI vendors like copilots or Bedrock agents), Sentra helps privacy and legal teams perform realistic transfer impact assessments and verify that technical safeguards (encryption, restricted access, logging) match contractual commitments. Reports can be exported to document compliance for internal review and external auditors.

Records of Processing, DPIAs, and Governance (Articles 24, 25, 30, 35–36)

GDPR Control / Obligation	How Sentra Helps
Controller Accountability & Responsibilities (Art. 24)	Sentra provides **continuous, evidence-based visibility** into where personal data resides, who can access it, and what security posture and exposure exist. This evidence underpins your ability, as controller or joint controller, to demonstrate appropriate measures and their effectiveness to supervisory authorities.
Privacy by Design and by Default (Art. 25)	Sentra enables teams to build and enforce privacy controls into their systems from day one, while ensuring default configurations minimize unnecessary data collection, retention, and access. In addition, Sentra continuously monitors changes across the data environment, helping ensure that newly introduced data stores, datasets, and processes adhere to Privacy by Design principles from the outset.

GDPR Control / Obligation	How Sentra Helps
Records of Processing Activities (RoPA) (Art. 30)	Sentra provides a comprehensive, continuously updated data inventory (RoPA) report that maps all data stores, sensitive data classifications, and access permissions—eliminating reliance on manual, error-prone inventory management. The report can be exported directly from Sentra and shared with governance teams and auditors to support compliance and streamline assessments.
Data Protection Impact Assessments (DPIAs) (Arts. 35–36)	For high-risk processing and AI projects, Sentra supplies the **data maps, sensitivity classifications, residency details, and risk scores** needed to complete DPIAs and, where applicable, Fundamental Rights Impact Assessments. Automated, **audit-ready reports** summarize data flows, AI usage, and applied controls, reducing the manual overhead of DPIA documentation.

Summary

This table-driven guide shows how Sentra's DSPM, DDR, DAG, and AI-aware capabilities support many of the **operational controls required by GDPR,** including:

- Core **principles** (lawfulness, minimization, storage limitation, integrity/confidentiality, accountability).
- **Data subject rights** and DSAR execution.
- **Security of processing** and breach response.
- **Data residency and international transfers.**
- **Records of processing, DPIAs, and privacy-by-design governance.**

Gartner Peer Insights Customers' Choice 2025™

Gartner® Peer Insights™

4.9 ★★★★★

By Sentra in Data Security Posture Management (DSPM)

Setting a New Standard in Data Security

>95% Accuracy

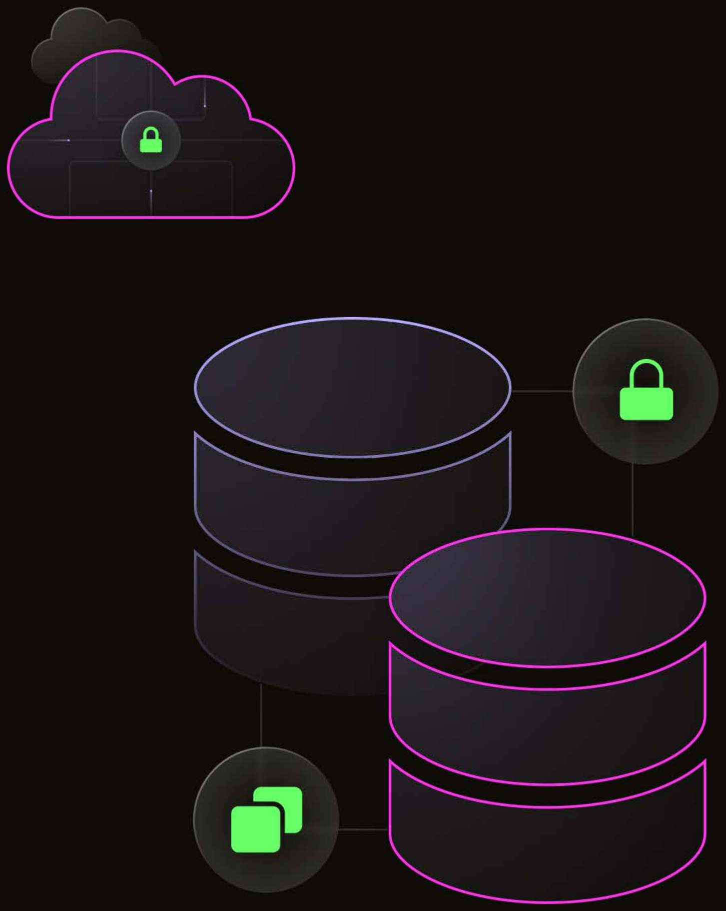
AI-powered classification

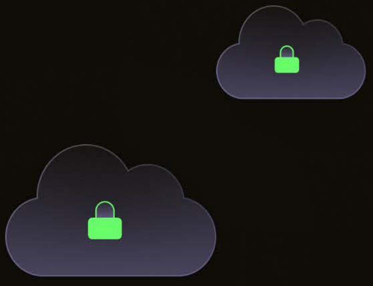
10x more efficient

In scanning compared to industry

In less than 1 week

Discover and assess data risks @ PB — scale





sentra

Visit www.sentra.io | **Watch a demo**

For more information, please contact us at info@sentra.io