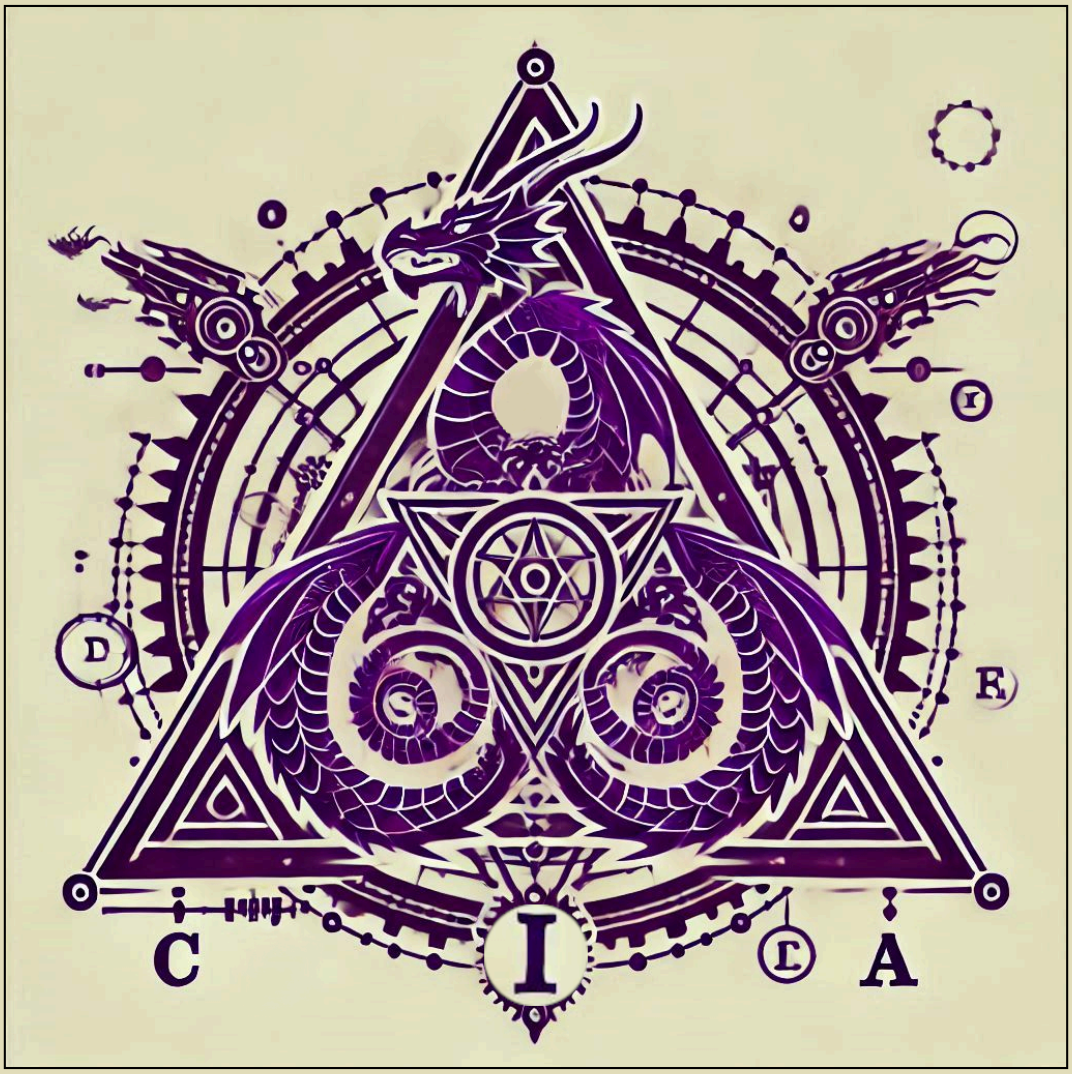
Unlocking GDPR

Purple Dragon Cybersecurity's Guide to Operationalizing GDPR



Summary of GDPR Articles

Article 1 - Subject-matter and objectives

Not an operational requirement. Outlines subject matter. Not operational for startups, but sets context.

Article 2 - Material scope

Required. Material scope of GDPR. Helps determine applicability — relevant.

Article 3 - Territorial scope

Required. Territorial scope. Highly relevant for non-EU startups with EU customers.

Article 4 - Definitions

Not an operational requirement. Definitions. Important for accurate interpretation, but not operationalized.

Article 5 - Principles relating to processing of personal data

Required. Core processing principles. Must be respected and documented by all controllers.

Article 6 - Lawfulness of processing

Required. Defines lawful bases for processing. You must identify and document one. Legal bases include: consent, contract, legal obligation, vital interests, public task, or legitimate interests.

Article 7 - Conditions for consent

Required. Conditions for valid consent. Applies if consent is your legal basis. Consent must be freely given, specific, informed, and unambiguous. Note: Other legal bases such as contract or legitimate interest may apply instead.

Article 8 - Conditions applicable to child's consent

Optional. Child consent. Applies only if your service targets children under 16 in the EU.

Article 9 - Processing of special categories of personal data

Required. Special category data (health, biometrics, etc). Needed if processing such data.

Article 10 - Processing of personal data relating to criminal convictions and offences

Not an operational requirement. Processing not requiring identification. Rarely applies to typical SaaS use cases.

Article 11 - Processing which does not require identification

Not an operational requirement. Situations where identification is unnecessary. Rarely invoked.

Article 12 - Transparent information, communication and modalities

Required. Transparency obligations. Key for privacy policies and notices.

Article 13 - Information to be provided where personal data are collected from the data subject

Required. Information to provide when collecting data from individuals. Core compliance duty.

Article 14 - Information to be provided where personal data have not been obtained from the data subject

Required. Information to provide when data is collected indirectly. Must be documented.

Article 15 - Right of access by the data subject

Required. Right of access. You must build a DSAR process.

Article 16 - Right to rectification

Required. Right to rectification. Systems should allow user correction.

Article 17 - Right to erasure ('right to be forgotten')

Required. Right to erasure. Relevant for deletion workflows.

Article 18 - Right to restriction of processing

Required. Right to restrict processing. DSAR variant — workflow required.

Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing

Required. Notification of rectification or erasure. Requires coordination across systems.

Article 20 - Right to data portability

Required. Right to data portability. Applies if you rely on consent or contract.

Article 21 - Right to object

Required. Right to object. Applies to marketing, profiling, etc.

Article 22 - Automated individual decision-making, including profiling

Optional. Automated decision-making. Applies only if using algorithms with legal effect.

Article 23 - Restrictions

Required. Legal grounds for restricting rights (e.g., law enforcement). Must be built into DSARs.

Article 24 - Responsibility of the controller

Required. Accountability. Requires demonstrating compliance — touches all governance.

Article 25 - Data protection by design and by default

Required. Privacy by design and by default. Engineering principle all teams must follow.

Article 26 - Joint controllers

Optional. Joint controllers. Required if shared decision-making occurs with partners.

Article 27 - Representatives of controllers or processors not established in the Union

Required. EU representative. Needed for non-EU orgs targeting EU citizens.

Article 28 - Processor

Required. Processor responsibilities. Required for vendor agreements.

Article 29 - Processing under the authority of the controller or processor

Not an operational requirement. Processor behavior. Reinforces Article 28 — not separately operationalized.

Article 30 - Records of processing activities

Required. Records of processing. Create a ROPA unless exempt.

Article 31 - Cooperation with the supervisory authority

Not an operational requirement. Cooperation with authorities. Relevant in audits or complaints.

Article 32 - Security of processing

Required. Security measures. Requires appropriate technical and organizational controls.

Article 33 - Notification of a personal data breach to the supervisory authority

Required. Breach notification to DPA. Must be operationalized.

Article 34 - Communication of a personal data breach to the data subject

Required. Breach notification to data subjects. Applies if breach risks harm.

Article 35 - Data protection impact assessment

Required. DPIAs. Applies to high-risk processing — templates recommended.

Article 36 - Prior consultation

Optional. Prior consultation. Applies only in very high-risk situations.

Article 37 - Designation of the data protection officer

Optional. Designation of DPO. May be optional, but recommended for enterprise maturity.

Article 38 - Position of the data protection officer

Optional. DPO independence and role. Applies only if you appoint one.

Article 39 - Tasks of the data protection officer

Optional. DPO responsibilities. Must be documented and supported.

Article 40 - Codes of conduct

Optional. Codes of conduct. Optional — useful for demonstrating accountability.

Article 41 - Monitoring of approved codes of conduct

Not an operational requirement. Monitoring of codes of conduct. Only relevant if enrolled in one.

Article 42 - Certification

Optional. Certification. Optional, helpful for sales/compliance but not required.

Article 43 - Certification bodies

Not an operational requirement. Accreditation of certification bodies. Not applicable to controllers/processors.

Article 44 - General principle for transfers

Required. Transfer principles. Must be followed for international data movement.

Article 45 - Transfers on the basis of an adequacy decision

Optional. Adequacy decisions. Permits frictionless transfer to some countries.

Article 46 - Transfers subject to appropriate safeguards

Required. Appropriate safeguards. Most startups rely on SCCs under this article.

Article 47 - Binding corporate rules

Optional. Binding corporate rules. Applies to large multinational groups.

Article 48 - Transfers or disclosures not authorised by Union law

Not an operational requirement. Third-country access. Describes issues with government data access.

Article 49 - Derogations for specific situations

Optional. Derogations. Emergency fallback basis for transfers.

Article 50 - International cooperation for the protection of personal data

Not an operational requirement. International cooperation. Not operationalized by private companies.

Article 51 - Supervisory authority

Optional. Supervisory authority. Know your lead DPA if operating in EU.

Article 52 - Independence

Not an operational requirement. Independence of authority. Not relevant to data controllers.

Article 53 - General conditions for the members of the supervisory authority

Not an operational requirement. General conditions for DPA members. Governance-level; not startup-facing.

Article 54 - Rules on the establishment of the supervisory authority

Not an operational requirement. Rules for DPA staff. Not operational.

Article 55 - Competence

Not an operational requirement. DPA competencies. Understand what they can enforce, but not actionable.

Article 56 - Competence of the lead supervisory authority

Not an operational requirement. Cross-border oversight. Applies if you're in multiple EU markets.

Article 57 - Tasks

Not an operational requirement. Tasks of DPA. Not operational for your business.

Article 58 - Powers

Not an operational requirement. DPA powers. Important to understand scope, but not implemented.

Article 59 - Activity reports

Not an operational requirement. Annual reports. Applies to DPAs, not private companies.

Article 60 - Cooperation between the lead supervisory authority and the other supervisory authorities concerned

Not an operational requirement. Cooperation among authorities. Not applicable.

Article 61 - Mutual assistance

Not an operational requirement. Mutual assistance. Government-level.

Article 62 - Joint operations of supervisory authorities

Not an operational requirement. Joint operations. Regulatory concept.

Article 63 - Consistency mechanism

Not an operational requirement. Consistency mechanism. Applies to regulators.

Article 64 - Opinion of the Board

Not an operational requirement. Board opinions. Regulatory guidance only.

Article 65 - Dispute resolution by the Board

Not an operational requirement. Dispute resolution by Board. Not business applicable.

Article 66 - Urgency procedure

Not an operational requirement. Urgency procedure. Legal procedural only.

Article 67 - Exchange of information

Not an operational requirement. Information exchange among DPAs. Not operational.

Article 68 - European Data Protection Board

Not an operational requirement. European Data Protection Board. Regulatory.

Article 69 - Independence of the Board
Not an operational requirement. Board members. Non-operational.

Article 70 - Tasks of the Board
Not an operational requirement. Board tasks. Context only.

Article 71 - Proceedings
Not an operational requirement. Board procedures. Not implemented by companies.

Article 72 - Chair
Not an operational requirement. Chair appointment. Not applicable.

Article 73 - Secrecy
Not an operational requirement. Board secrecy rules. Governmental.

Article 74 - Tasks of the Commission
Not an operational requirement. Commission role. Not for startups.

Article 75 - Committee procedure
Not an operational requirement. Committee procedure. Institutional.

Article 76 - Exercise of the delegation
Not an operational requirement. Exercise of delegation. Procedural.

Article 77 - Right to lodge a complaint with a supervisory authority
Required. Right to lodge a complaint. Must inform users in privacy policy.

Article 78 - Right to an effective judicial remedy against a supervisory authority
Not an operational requirement. Right to judicial remedy vs. DPA. Legal risk awareness.

Article 79 - Right to an effective judicial remedy against a controller or processor
Not an operational requirement. Right to remedy vs. controller. Legal exposure; defensibility matters.

Article 80 - Representation of data subjects
Not an operational requirement. Representation of data subjects. Not directly operationalized.

Article 81 - Suspension of proceedings
Not an operational requirement. Proceedings suspension. Court procedure.

Article 82 - Right to compensation and liability
Not an operational requirement. Compensation. Drives need for defensible governance.

Article 83 - General conditions for imposing administrative fines

Not an operational requirement. Administrative fines. Sets stakes for enforcement.

Article 84 - Penalties

Not an operational requirement. Criminal penalties. Depends on local member state law.

Article 85 - Processing and freedom of expression and information

Not an operational requirement. Freedom of expression. Legal carveout — not a startup control.

Article 86 - Processing and public access to official documents

Not an operational requirement. Access to public documents. Applies to public bodies.

Article 87 - Processing of the national identification number

Optional. National ID numbers. Only if you collect such data.

Article 88 - Processing in the context of employment

Optional. Employment context. Local law carveouts.

Article 89 - Safeguards and derogations for archiving, research and statistics

Optional. Research and archiving. Special rules; not most startups.

Article 90 - Obligations of secrecy

Not an operational requirement. Secrecy obligations. Only for regulated professions.

Article 91 - Existing data protection rules of churches and religious associations

Not an operational requirement. Church data handling. Not relevant.

Article 92 - Exercise of the delegation

Not an operational requirement. Commission powers. Procedural.

Article 93 - Committee procedure

Not an operational requirement. Committee rules. Not applicable.

Article 94 - Repeal of Directive 95/46/EC

Not an operational requirement. Directive repeal. Contextual only.

Article 95 - Relationship with ePrivacy Directive

Optional. ePrivacy regulation. Separate law — still relevant.

Article 96 - Relationship with previously concluded agreements

Not an operational requirement. Relationship with third countries. Policy level.

Article 97 - Commission reports

Not an operational requirement. Commission reports. Informational.

Article 98 - Review of other Union legal acts

Not an operational requirement. Entry into force. Historical.

Article 99 - Entry into force and application

Not an operational requirement. Application start date. Reference only.

Not an operational requirement.

Operationalizing GDPR Requirements

Article 5 – Principles relating to processing of personal data

Purpose & Scope

Article 5 lays out the core principles that underlie all GDPR-compliant processing activities. It forms the philosophical foundation of the entire regulation.

Compliance Triggers

- All personal data processing activities in your organization
- Privacy policy creation and updates
- Data mapping, DPIAs, and vendor reviews

What to Document

- Demonstrable adherence to principles: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability
- Retention schedules and minimization controls
- Security measures and governance records

Enterprise Diligence Expectations

Customers and regulators may expect narrative explanations or policy excerpts showing how these principles are operationalized.

Practical Guidance

- Use these principles as privacy design pillars
- Translate them into system-level rules (e.g., purpose tags, deletion logic, etc.)
- In audits, be ready to map internal processes to each of these principles

Article 6 – Lawfulness of processing

Purpose & Scope

Article 6 defines the legal bases on which personal data may be lawfully processed under the GDPR.

Compliance Triggers

- Collection or processing of any personal data under GDPR scope
- Evaluating if processing has a valid legal basis (e.g. consent, contract, legal obligation, vital interests, public task, or legitimate interests)

What to Document

- Mapping of each processing activity to a valid legal basis
- Justification and records of legitimate interest assessments (if applicable)
- Consent records, contracts, or references to applicable laws

Enterprise Diligence Expectations

B2B partners will expect to see a legal basis tied to each category of processing in your ROPA or privacy policy.

Practical Guidance

- Build a master data processing inventory and legal basis map
- Use standard templates for Legitimate Interest Assessments
- Review basis regularly, especially if processing changes

Article 7 – Conditions for consent

Purpose & Scope

Article 7 outlines the conditions that make consent valid under GDPR, including that it must be freely given, specific, informed, and unambiguous.

Compliance Triggers

- Using consent as the legal basis for processing
- Obtaining consent from users, customers, or employees

What to Document

- Consent request design (UX or form screenshots)
- Audit logs of consent grants and withdrawals
- Policy for responding to consent withdrawal requests

Enterprise Diligence Expectations

Buyers may request sample consent language and proof of granular opt-in/out capabilities.

Practical Guidance

- Avoid bundling consent with other terms
- Make it as easy to withdraw as it is to give consent
- Store consent in a structured and queryable format

Article 9 – Processing of special categories of personal data

Purpose & Scope

Article 9 prohibits the processing of special category data unless specific exceptions apply. This includes racial/ethnic origin, political opinions, religious beliefs, health data, biometrics, and more.

Compliance Triggers

- Processing biometric, health, or racial data
- AI/ML models involving sensitive classifications
- Medical, HR, or accessibility features

What to Document

- Lawful basis AND Article 9 exemption used (explicit consent, legal obligation, etc.)
- Risk mitigation and security measures
- Purpose-specific limitations and access controls

Enterprise Diligence Expectations

Customers may ask whether you process special category data and how it's protected. Absence of this data type should be affirmatively stated in some assessments.

Practical Guidance

- Avoid processing if not absolutely necessary
- Use data minimization or anonymization when possible
- Ensure explicit consent UI meets GDPR standards if consent is used

Article 11 – Processing which does not require identification

Purpose & Scope

Article 11 clarifies that controllers are not required to maintain or obtain additional information to identify a data subject if they don't already possess such identifiers.

Compliance Triggers

- Anonymous or pseudonymous data processing
- Requests for access or erasure where the controller cannot reasonably identify the data subject

What to Document

- Policy for verifying identity of data subjects
- Records of anonymization or pseudonymization practices
- Justification for when identification is not pursued

Enterprise Diligence Expectations

Buyers may ask whether your privacy program includes controls to avoid unnecessary data linkage or re-identification.

Practical Guidance

- Avoid collecting more personal data than necessary just to fulfill rights requests
- Maintain a decision log for identity verification practices
- Use this article to reduce friction in low-risk processing cases

Article 12 – Transparent Information, Communication and Modalities

Purpose & Scope

Article 12 ensures data subjects receive information in a clear, concise, and accessible format. This article underpins transparency obligations across Articles 13–22.

Compliance Triggers

- Publishing or updating a privacy policy
- Responding to DSARs (access, rectification, erasure)
- Designing consent or objection workflows

What to Document

- Policies written in plain language
- Multichannel delivery (web, app, print, etc.)
- Translation/localization for different audiences
- Processes to respond without undue delay

Enterprise Diligence Expectations

Reviewers expect to see well-structured, easily accessible privacy policies and transparency mechanisms across the UX.

Practical Guidance

- Use layered notices (e.g., short + full versions)
- Avoid burying privacy info in dense T&Cs
- Include contact details and how rights can be exercised

Article 13 – Information to be provided where personal data are collected from the data subject

Purpose & Scope

Article 13 requires that data subjects are informed at the time their data is collected. The notice must include identity of the controller, purposes, lawful basis, recipients, rights, and more.

Compliance Triggers

- User signup flows
- Form submissions
- Mobile app data collection

What to Document

- What data is collected and why
- Your lawful basis (linked to Article 6)
- Retention period, contact info, right to withdraw consent

Enterprise Diligence Expectations

Enterprise customers expect concise but complete disclosures visible at or before data collection.

Practical Guidance

- Embed privacy notices near the point of interaction
- Audit marketing forms for compliance regularly
- Localize per user region if needed

Article 14 – Information where personal data have not been obtained from the data subject

Purpose & Scope

Article 14 mandates that individuals are informed when their data is obtained indirectly. This ensures transparency in cases like third-party data enrichment or referrals.

Compliance Triggers

- B2B contact enrichment
- Purchased lead lists
- Referrals or scraped public data

What to Document

- How and where data was obtained
- Planned use and data categories
- Legal basis and notification timing

Enterprise Diligence Expectations

Larger customers may ask about third-party sourcing practices and if Article 14 notices are sent.

Practical Guidance

- Automate notification emails for indirect collection
- Disclose data sourcing in privacy policy
- Track exemptions when providing notice is impossible

Article 15 – Right of access

Purpose & Scope

Article 15 grants data subjects the right to obtain confirmation and access to their personal data and related processing details.

Compliance Triggers

- Receipt of a Data Subject Access Request (DSAR)
- Internal audits or vendor assessments involving data rights

What to Document

- DSAR intake process and template response
- Proof of identity verification protocol
- System logs showing data sources and access scope

Enterprise Diligence Expectations

Buyers often ask how you handle DSARs — turnaround time, identity checks, exclusions, and logging.

Practical Guidance

- Develop a DSAR workflow with internal SLAs
- Use templated responses but tailor per request
- Ensure data includes metadata, processing purposes, and categories

Article 16 – Right to Rectification

Purpose & Scope

Article 16 gives individuals the right to have inaccurate personal data corrected without undue delay.

Compliance Triggers

- DSAR requesting correction
- User-submitted profile updates
- CRM or HR record discrepancies

What to Document

- Correction procedures and validation rules
- Version history (if applicable)
- How rectification is communicated to third parties

Enterprise Diligence Expectations

Customers may ask about your rectification flow and how you verify legitimacy of changes.

Practical Guidance

- Allow self-service correction when possible
- Audit logs of changes may be needed for disputes
- Sync corrections across downstream systems

Article 17 – Right to Erasure ('Right to be Forgotten')

Purpose & Scope

Article 17 allows individuals to request deletion of their personal data under specific conditions, such as consent withdrawal or unlawful processing.

Compliance Triggers

- DSAR requesting deletion
- Account closure
- Retention schedule expiry

What to Document

- Deletion workflows across systems and backups
- Conditions under which requests are denied (e.g. legal obligation)
- Time to fulfillment and exceptions

Enterprise Diligence Expectations

Partners may request a sample policy or description of how deletion cascades through your stack.

Practical Guidance

- Implement data tagging for deletion eligibility
- Have a 'partial delete' model if required (e.g., for logs)
- Communicate clearly if deletion is delayed or denied

Article 18 – Right to Restriction of Processing

Purpose & Scope

Article 18 allows individuals to restrict the use of their data while disputes are being resolved or when processing is unlawful but erasure isn't requested.

Compliance Triggers

- Challenge to data accuracy or lawfulness
- DSAR requesting restriction
- Litigation hold

What to Document

- Conditions that justify restriction
- System capabilities to mark data as restricted
- Notifications to recipients of restricted status

Enterprise Diligence Expectations

Auditors may ask whether your systems allow granular data status changes and what 'restriction' actually looks like in practice.

Practical Guidance

- Tag restricted records in your DBs or CRM
- Pause automated flows (marketing, analytics)
- Document how restricted status is lifted

Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing

Purpose & Scope

Article 19 ensures that any rectification, erasure, or restriction of personal data is communicated to all recipients of that data. It reinforces transparency and data lifecycle accountability.

Compliance Triggers

- A data subject exercises their right to rectification (Article 16), erasure (Article 17), or restriction (Article 18)
- Third-party vendors or sub-processors hold affected data

What to Document

- Notification procedures for downstream recipients
- Automated tracking of data subject request propagation
- Audit log confirming notice delivery or attempted contact

Enterprise Diligence Expectations

Business partners may ask how you ensure rectifications and deletions cascade to processors or shared services.

Practical Guidance

- Maintain a recipient registry for shared data
- Implement automated flags in your CRM or data pipeline
- Create a templated notification for Article 19 updates

Article 20 – Right to data portability

Purpose & Scope

Article 20 gives individuals the right to receive their personal data in a structured, commonly used format and to transmit it to another controller.

Compliance Triggers

- DSAR requesting export
- Account migration or transfer
- New product onboarding with import option

What to Document

- Supported data formats (e.g., JSON, CSV)
- Authentication and security procedures for export
- Policy for responding to portability requests within one month

Enterprise Diligence Expectations

Some SaaS customers will ask whether users can export their data and how long the process takes.

Practical Guidance

- Provide a self-service export option where possible
- Include metadata and relationships if meaningful (e.g., timestamps, preferences)
- Log fulfillment date and format used

Article 21 – Right to object

Purpose & Scope

Article 21 allows data subjects to object to processing based on legitimate interest or for direct marketing.

Compliance Triggers

- Use of personal data for behavioral ads or profiling
- Processing based on legitimate interest instead of consent

What to Document

- Opt-out mechanism
- Assessment of legitimate interest override (balancing test)
- Communication and tracking of objection outcomes

Enterprise Diligence Expectations

Reviewers may expect to see where users can opt out and how that preference is enforced.

Practical Guidance

- Provide one-click opt-out from marketing emails
- Track opt-out status centrally and honor it globally
- Document why processing continues if objection is denied

Article 22 – Automated individual decision-making, including profiling

Purpose & Scope

Article 22 restricts decisions based solely on automated processing that produce legal or similarly significant effects on individuals.

Compliance Triggers

- Use of AI/ML to approve/deny applications
- Automated hiring or lending decisions
- Dynamic pricing or personalization engines

What to Document

- Nature of automated decision-making
- Safeguards in place (e.g., human review)
- How data subjects can request explanation or intervention

Enterprise Diligence Expectations

Companies using automation must be transparent about its role in decisions. B2B clients may request a policy or whitepaper.

Practical Guidance

- Include Article 22 analysis in your DPIA
- Offer manual override or review channel
- Explain algorithmic logic in user-facing disclosures where applicable

Article 23 – Restrictions

Purpose & Scope

Article 23 permits EU member states to restrict the scope of data subject rights in specific situations, such as national security, criminal investigations, or public interest.

Compliance Triggers

- Situations where access to data or fulfillment of rights requests must be limited or deferred
- Sector-specific scenarios (e.g., finance, law enforcement, health)

What to Document

- Policy defining lawful bases for restricting access
- Exemption scenarios and procedures for review
- Template language for responding to restricted DSARs

Enterprise Diligence Expectations

Buyers may inquire about how your system handles DSAR denials and whether your restrictions are lawful and logged.

Practical Guidance

- Integrate logic into your DSAR workflow to handle restrictions
- Train privacy responders on how to assess and justify exemptions
- Reference national law explicitly in denial communications

Article 24 – Responsibility of the controller

Purpose & Scope

Article 24 holds the controller accountable for GDPR compliance and mandates appropriate data protection measures by design and default.

Compliance Triggers

- Any organization acting as a controller of personal data
- Establishing privacy programs, roles, and controls

What to Document

- Privacy policies and governance procedures
- Risk assessments and technical/organizational safeguards
- Assignment of roles (DPO, privacy contact)

Enterprise Diligence Expectations

Auditors and enterprise buyers want to see proactive accountability — not just reactive responses.

Practical Guidance

- Map key responsibilities to roles internally
- Align controller responsibilities with ISO 27001/27701 if possible
- Use a dashboard to track policy implementation and controls

Article 25 – Data protection by design and by default

Purpose & Scope

Article 25 requires data protection measures to be embedded into the design of systems, products, and services — not bolted on afterward.

Compliance Triggers

- Design of new products or features
- Major system redesign or integration of third-party platforms

What to Document

- Privacy Impact Assessments (PIAs or DPIAs) during design phase
- Default configurations that minimize personal data usage
- Design choices for user control and transparency

Enterprise Diligence Expectations

Sophisticated customers will ask about 'data minimization by design' — especially in RFPs or DPIAs.

Practical Guidance

- Document default settings (e.g., off-by-default tracking)
- Have checklists for product launches that tie to Article 25
- Involve privacy or security reviews in early feature design

Article 26 – Joint controllers

Purpose & Scope

Article 26 governs situations where two or more controllers jointly determine the purposes and means of processing — requiring a transparent allocation of responsibilities.

Compliance Triggers

- Shared platforms or integrations where partners co-determine processing
- Collaborative data initiatives involving two or more entities

What to Document

- Joint controller arrangement agreements
- Public-facing summary of role split (typically in a privacy policy)
- Mechanism to handle data subject rights jointly

Enterprise Diligence Expectations

Buyers will expect a clearly articulated role model: joint controller, independent controller, or processor?

Practical Guidance

- Use a template agreement for joint control situations
- Coordinate contact points for rights requests
- Ensure accountability is not ambiguous in operations

Article 27 – Representatives of controllers or processors not in the EU

Purpose & Scope

Article 27 requires non-EU companies subject to GDPR to appoint a representative in the EU for contact by regulators and data subjects.

Compliance Triggers

- Offering goods/services to EU residents
- Monitoring behavior of individuals in the EU
- Company lacks physical presence in the EU

What to Document

- Designation of representative (name, contact info, EU location)
- Contract outlining scope and responsibilities
- Inclusion of representative info in privacy notice

Enterprise Diligence Expectations

Buyers may verify that you have an EU representative when no presence exists inside the EU.

Practical Guidance

- Maintain an up-to-date EU representative agreement
- Ensure clear internal contact path for regulator inquiries
- Choose a representative with GDPR experience

Article 28 – Processor obligations

Purpose & Scope

Article 28 outlines mandatory contractual terms between controllers and processors (vendors) to ensure GDPR-aligned handling of personal data.

Compliance Triggers

- Working with any third party that processes personal data on your behalf
- Updating or creating new vendor contracts

What to Document

- Data Processing Agreements (DPAs) with required clauses
- Vendor vetting and onboarding practices
- List of sub-processors and notification methods

Enterprise Diligence Expectations

Buyers expect to see Article 28-compliant DPAs and sub-processor disclosures.

Practical Guidance

- Maintain a signed DPA for every data processor
- Pre-approve sub-processor lists in contract addenda
- Review and renew vendor assessments annually

Article 30 – Records of processing activities (ROPA)

Purpose & Scope

Article 30 requires controllers and processors to maintain a record of all processing activities under their responsibility, unless exempt under specific conditions.

Compliance Triggers

- Employing 250+ people OR processing data regularly and non-occasionally
- Processing sensitive data or data that poses risks

What to Document

- List of processing activities by purpose, data category, recipient, and retention schedule
- Transfers to third countries and legal bases
- Technical and organizational security measures

Enterprise Diligence Expectations

Most enterprise buyers will ask for a copy of your ROPA or expect the information to be readily available.

Practical Guidance

- Start with a spreadsheet or table with columns per Article 30(1) and (2)
- Map systems and subprocessors into the ROPA
- Review and update quarterly, especially as features or vendors change

Article 32 – Security of processing

Purpose & Scope

Article 32 requires appropriate technical and organizational security measures to protect personal data against unauthorized access, loss, or damage.

Compliance Triggers

- Handling sensitive or high-volume personal data
- Incident response or breach handling
- New system launch or cloud migration

What to Document

- Access controls, encryption, backup procedures
- Risk assessments (technical + organizational)
- Security incident response policies

Enterprise Diligence Expectations

Customers want to see evidence of a security program aligned with ISO 27001, SOC 2, or similar.

Practical Guidance

- Map security controls to risks specific to your data and industry
- Keep technical measures updated (e.g., TLS versions, EDR coverage)
- Perform tabletop exercises and retain logs of past incidents

Article 33 – Notification of a personal data breach to the supervisory authority

Purpose & Scope

Article 33 requires controllers to notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach.

Compliance Triggers

- Confirmed or suspected personal data breach
- Security incident affecting confidentiality, integrity, or availability of personal data

What to Document

- Breach notification policy and process
- Timeline of breach detection and response
- Communications with the authority, including justification if delayed

Enterprise Diligence Expectations

Enterprise partners want to know you can meet tight breach reporting windows and have a well-rehearsed plan.

Practical Guidance

- Include GDPR breach criteria in your IR playbook
- Ensure breach impact assessment templates are ready
- Keep records of all notifications and rationale for any delays

Article 34 – Communication of a personal data breach to the data subject

Purpose & Scope

Article 34 requires you to notify affected individuals directly if a data breach is likely to result in a high risk to their rights and freedoms.

Compliance Triggers

- Confirmed breach with risk of identity theft, discrimination, financial loss, or reputational harm
- Loss of unencrypted sensitive data

What to Document

- Criteria used to assess whether notification is required
- Template language and approved communication channels
- Any justification for relying on an Article 34(3) exemption

Enterprise Diligence Expectations

Customers may review your breach communication plan or request to see anonymized examples of past messages.

Practical Guidance

- Maintain pre-approved breach comms templates
- Align your risk threshold with supervisory guidance
- Document each communication event for audit trail purposes

Article 35 – Data Protection Impact Assessments (DPIAs)

Purpose & Scope

Article 35 mandates that DPIAs be carried out when processing is likely to result in a high risk to individuals, especially for new technologies, large-scale monitoring, or profiling.

Compliance Triggers

- Launching a new feature involving sensitive or behavioral data
- Conducting large-scale surveillance, automated decisions, or systematic monitoring

What to Document

- Nature, scope, and purpose of processing
- Assessment of risks to rights and freedoms
- Measures taken to address those risks
- Outcome of consultation with DPO or supervisory authority, if any

Enterprise Diligence Expectations

Expect scrutiny around high-risk projects — buyers will ask if DPIAs were done and what resulted.

Practical Guidance

- Create a short DPIA template that any product or legal team can fill out
- Maintain a DPIA log, even if most result in 'low risk' conclusions
- Link DPIA completion to product launch or procurement workflows

Article 37 – Designation of the Data Protection Officer (DPO)

Purpose & Scope

Article 37 outlines when organizations must designate a Data Protection Officer (DPO), particularly when core activities involve large-scale processing of sensitive data or monitoring.

Compliance Triggers

- Large-scale processing of special categories of data
- Regular and systematic monitoring of individuals
- Public authorities or bodies

What to Document

- DPO designation and contact information
- DPO's qualifications and role description
- Evidence of independence and reporting line to top management

Enterprise Diligence Expectations

B2B partners may ask who your DPO is, how they're resourced, and whether they can operate independently.

Practical Guidance

- If no DPO is required, designate a privacy contact and explain why a formal DPO isn't mandated
- Ensure the DPO is consulted early in privacy-impacting decisions
- Document DPO involvement in audits, DPIAs, and compliance reviews

Article 38 – Position of the Data Protection Officer

Purpose & Scope

Article 38 governs the organizational positioning of the DPO, emphasizing independence, access to leadership, and resources to perform their role effectively.

Compliance Triggers

- Formal designation of a DPO
- Embedding privacy governance within corporate structure

What to Document

- Reporting line of DPO to senior management
- Conflict of interest assessment for the DPO's role
- Policies protecting DPO from dismissal or penalty for performing duties

Enterprise Diligence Expectations

Buyers may review how independent your DPO truly is — whether they can challenge decisions and have executive access.

Practical Guidance

- Avoid assigning the DPO role to someone with competing interests (e.g., head of security or compliance)
- Give DPO authority and visibility in risk assessments and product reviews
- Encourage ongoing professional development

Article 39 – Tasks of the Data Protection Officer

Purpose & Scope

Article 39 defines the responsibilities of the DPO, including monitoring compliance, training staff, and serving as a contact point for data subjects and regulators.

Compliance Triggers

- Ongoing GDPR accountability and lifecycle management
- Engagement with supervisory authorities

What to Document

- Internal audit schedules or reports led by the DPO
- Privacy training materials and attendance records
- Correspondence log with data subjects or DPAs

Enterprise Diligence Expectations

Buyers will expect evidence that your DPO is involved in practical oversight — not just a name on paper.

Practical Guidance

- Have the DPO maintain a compliance calendar and action log
- Build a DSAR and breach-handling workflow with DPO participation
- Use quarterly reviews to track DPO engagement

Article 40 – Codes of conduct

Purpose & Scope

Article 40 encourages the creation and adoption of codes of conduct by industry associations to help interpret and apply GDPR principles contextually.

Compliance Triggers

- Membership in an industry group with an approved code
- Desire to demonstrate accountability or compliance posture

What to Document

- Membership or adoption of relevant codes
- Internal training or enforcement based on the code
- Demonstrated alignment with best practices

Enterprise Diligence Expectations

Buyers may ask if you adhere to any sector-specific standards or participate in any GDPR-aligned industry initiatives.

Practical Guidance

- Monitor sector-specific GDPR codes relevant to your industry
- Map code provisions to internal policies
- Use adherence as a supporting control in audits

Article 41 – Monitoring of approved codes of conduct

Purpose & Scope

Article 41 allows for the accreditation of monitoring bodies that oversee compliance with approved codes of conduct.

Compliance Triggers

- Participation in a monitored code of conduct
- Reliance on monitored adherence as a safeguard or compliance measure

What to Document

- Details of monitoring body accreditation
- Internal compliance audit trail under the code
- Disciplinary procedures for non-compliance

Enterprise Diligence Expectations

This is relevant if you are relying on such mechanisms in your privacy posture — especially for small/midsize vendors.

Practical Guidance

- Know whether your code of conduct is monitored or just voluntary
- Document compliance activities to meet monitoring standards
- Use findings to strengthen internal policies

Article 42 – Certification

Purpose & Scope

Article 42 encourages the establishment of certification mechanisms to help demonstrate compliance — though formal GDPR certifications are still emerging.

Compliance Triggers

- Seeking GDPR-aligned certifications (e.g., Europrivacy)
- Use of certifications in vendor management or sales enablement

What to Document

- Certificates held, scope, and issuing body
- Controls mapped to certification requirements
- Renewal dates and audit findings

Enterprise Diligence Expectations

B2B buyers may ask if you're certified under any GDPR-aligned frameworks, even if not formally mandated.

Practical Guidance

- Track developments around Europrivacy and local schemes
- Use ISO 27001, SOC 2, or similar as interim proxies
- Maintain central repository of all certs and attestations

Article 43 – Certification bodies

Purpose & Scope

Article 43 governs the accreditation and role of certification bodies responsible for issuing GDPR-aligned certifications (e.g., Europrivacy).

Compliance Triggers

- Engagement with a GDPR certification body
- Pursuit of formal privacy certifications

What to Document

- Name and credentials of certification body
- Accreditation status from supervisory authority
- Certification scope and results

Enterprise Diligence Expectations

Buyers may ask whether your certifications are granted by a recognized body and if renewal/oversight mechanisms are in place.

Practical Guidance

- Choose an accredited body with recognized standing (e.g., under ENISA or national authority)
- Document each step of the certification process
- Track expiration and recertification dates

Article 44 – General principle for data transfers

Purpose & Scope

Article 44 establishes the overarching principle that any personal data transfer outside the EU must maintain equivalent protection as under the GDPR.

Compliance Triggers

- Transfers of data to countries outside the EU/EEA
- Use of third-party vendors or tools hosted outside the EU

What to Document

- Inventory of data transfers to third countries
- Transfer mechanism (e.g., SCCs, adequacy, BCRs)
- Assessment of local legal risks

Enterprise Diligence Expectations

Expect questions on how you legally justify international transfers and what safeguards you apply.

Practical Guidance

- Tag systems that trigger international transfers
- Prepare a one-pager explaining your legal basis for exports
- Monitor European Data Protection Board guidance on transfers

Article 45 – Transfers on the basis of an adequacy decision

Purpose & Scope

Article 45 permits data transfers to countries officially deemed to provide adequate protection by the European Commission.

Compliance Triggers

- Use of cloud or processing vendors based in countries with adequacy status (e.g., Japan, UK, Canada - limited)

What to Document

- Adequacy mapping to vendor geolocation
- Contractual acknowledgment of reliance on adequacy

Enterprise Diligence Expectations

Due diligence may include verifying vendor country status or adequacy reliance.

Practical Guidance

- Maintain an updated list of adequate jurisdictions
- Include adequacy rationale in vendor onboarding docs
- Don’t assume adequacy—double-check regional applicability

Article 46 – Transfers subject to appropriate safeguards

Purpose & Scope

Article 46 enables data transfers to non-adequate countries where appropriate safeguards are used, such as Standard Contractual Clauses (SCCs).

Compliance Triggers

- Transfers to US-based or non-adequate country vendors
- Reliance on SCCs or Binding Corporate Rules (BCRs)

What to Document

- Signed SCCs or other legal safeguards
- Transfer Impact Assessments (TIAs)
- Supplementary measures (e.g., encryption, access controls)

Enterprise Diligence Expectations

B2B customers expect documented evidence of your SCCs, TIAs, and an understanding of Schrems II compliance.

Practical Guidance

- Centralize executed SCCs and TIAs
- Keep logs of vendor legal evaluations
- Follow EDPB-recommended supplementary safeguards

Article 47 – Binding corporate rules (BCRs)

Purpose & Scope

Article 47 allows multinational companies to transfer personal data internally across borders using approved Binding Corporate Rules (BCRs).

Compliance Triggers

- International data transfers within corporate group
- Desire to avoid repetitive SCC signing between entities

What to Document

- Approved BCRs and supervisory authority decision
- List of covered entities and scope of applicability
- Internal enforcement and training procedures

Enterprise Diligence Expectations

Buyers may ask if your BCRs are approved and what oversight mechanisms are in place.

Practical Guidance

- BCRs are resource-intensive but simplify transfers at scale
- BCR documentation must include audit, complaint handling, and liability provisions
- Track approval dates and relevant jurisdictions

Article 48 – Transfers not authorized by Union law

Purpose & Scope

Article 48 clarifies that foreign court orders or administrative requests (e.g. subpoenas) do not override GDPR unless based on international agreement.

Compliance Triggers

- Receipt of foreign legal request for personal data
- Litigation or law enforcement demands from non-EU countries

What to Document

- Policy for evaluating cross-border legal requests
- Referral process to legal counsel
- Basis for disclosure or refusal

Enterprise Diligence Expectations

Customers — especially in regulated sectors — want to ensure you resist overbroad foreign requests and follow due process.

Practical Guidance

- Train staff to escalate all foreign disclosure demands
- Involve counsel immediately and assess against Article 48
- Document rejections or disclosures with legal justification

Article 49 – Derogations for specific situations

Purpose & Scope

Article 49 permits limited, exceptional transfers when other mechanisms are not available — e.g. explicit consent, contract necessity, or legal claims.

Compliance Triggers

- Urgent or one-time transfers to non-adequate countries
- Lack of SCCs or BCRs

What to Document

- Legal basis for derogation (e.g., consent, legal defense)
- Documentation that the transfer is not repetitive or systemic
- Transparency notices to affected individuals

Enterprise Diligence Expectations

Due diligence may include review of how often Article 49 is used and whether it's being abused as a fallback.

Practical Guidance

- Avoid relying on Article 49 unless strictly necessary
- Ensure fallback use is supported by documentation and warnings
- Keep consent logs and risk justifications

Article 51 – Supervisory authority

Purpose & Scope

Article 51 mandates that each EU Member State must establish one or more independent public authorities (DPAs) to enforce GDPR.

Compliance Triggers

- Processing operations involving multiple jurisdictions
- Questions of regulatory oversight, complaint handling, or enforcement

What to Document

- Lead supervisory authority (for companies with cross-border processing)
- Point of contact for regulatory communications
- Internal escalation protocol for DPA inquiries

Enterprise Diligence Expectations

Buyers — especially in the EU — often ask which DPA you are subject to and how you manage engagement.

Practical Guidance

- Identify and document your lead authority under the One-Stop-Shop principle
- Prepare internal guidance on regulator interaction
- Respond promptly to all communications from DPAs

Article 77 – Right to lodge a complaint with a supervisory authority

Purpose & Scope

Article 77 guarantees that individuals can lodge a complaint with a data protection authority if they believe their rights under GDPR have been violated.

Compliance Triggers

- Unresolved or denied data subject requests
- Data subject explicitly notifies your company of intent to escalate

What to Document

- Internal complaint handling procedures
- Contact details for supervisory authority provided in privacy notice
- Logged interactions and escalation paths

Enterprise Diligence Expectations

Buyers may ask if you clearly inform data subjects of their rights to complain and how you respond to such notices.

Practical Guidance

- Include clear contact paths in your privacy policy
- Ensure support staff know how to handle complaints respectfully
- Have template responses and escalation SOPs prepared

Article 78 – Right to an effective judicial remedy against a supervisory authority

Purpose & Scope

Article 78 provides recourse for individuals who believe a supervisory authority has not handled their complaint properly or within a reasonable timeframe.

Compliance Triggers

- Involvement in a regulatory investigation
- Regulator fails to respond to a complaint involving your company

What to Document

- Communication history with supervisory authorities
- Legal representation contacts and protocols for appeal handling

Enterprise Diligence Expectations

Though rarely triggered directly, buyers may ask how you interact with supervisory authorities.

Practical Guidance

- Ensure all regulator communications are archived and time-stamped
- Document outcomes and response delays to protect appeal rights
- Be aware of your lead authority under the One-Stop-Shop mechanism

Article 79 – Right to an effective judicial remedy against a controller or processor

Purpose & Scope

Article 79 empowers data subjects to bring legal proceedings directly against controllers or processors when GDPR rights have been violated.

Compliance Triggers

- Allegation of non-compliance raised by a data subject
- Service of legal notice from a data subject or regulator

What to Document

- Internal escalation process for handling GDPR claims
- Insurance coverage or legal representation for privacy disputes
- Timelines and tracking of legal response

Enterprise Diligence Expectations

In vendor reviews, customers may ask whether you've ever been the subject of GDPR litigation or how you'd handle it.

Practical Guidance

- Work with counsel to define litigation intake and response timelines
- Maintain confidentiality logs and investigation procedures
- Document how you will demonstrate compliance during proceedings

Article 82 – Right to compensation and liability

Purpose & Scope

Article 82 gives individuals the right to seek compensation if they suffer material or non-material damage due to GDPR infringements.

Compliance Triggers

- Confirmed breach or violation affecting data subjects
- Individual claims damage as a result of non-compliance

What to Document

- Claim intake procedures
- Legal liability coverage (e.g., cyber insurance)
- Assessment of harm and remediation offered

Enterprise Diligence Expectations

Buyers may want to understand how liability is allocated and whether the vendor maintains insurance.

Practical Guidance

- Maintain a record of any compensation requests
- Align incident logs with impact assessments
- Keep track of regulator-reported damages

Article 83 – General conditions for imposing administrative fines

Purpose & Scope

Article 83 outlines how and when fines may be imposed under GDPR, including criteria for assessment and maximum thresholds.

Compliance Triggers

- Confirmed GDPR violations
- Findings issued by supervisory authority

What to Document

- Record of decisions involving fines or warnings
- Mitigation actions taken post-finding
- Evidence of prior compliance efforts and good faith cooperation

Enterprise Diligence Expectations

Buyers may be interested in your enforcement history and approach to mitigating penalty risk.

Practical Guidance

- Ensure DPIAs, RoPA, and vendor contracts are well documented
- Maintain audit trails and change logs
- Engage with authorities constructively to demonstrate accountability

Article 84 – Penalties

Purpose & Scope

Article 84 enables Member States to lay down additional penalties beyond administrative fines, such as criminal sanctions for GDPR violations.

Compliance Triggers

- Local implementation laws imposing civil or criminal penalties
- Serious or repeat violations of national-level obligations

What to Document

- Mapping of national data protection laws to internal policies
- Awareness of additional legal risks beyond EU-level enforcement

Enterprise Diligence Expectations

This article is often more relevant to legal counsel, but serious buyers may ask about local legal exposures.

Practical Guidance

- Coordinate with counsel to track Member State variations
- Include localized requirements in privacy training and playbooks
- Monitor DPAs and industry associations for regulatory trends