CHECKLIST

GDPR Compliance Checklist

69 actionable items across 10 categories — lawful basis, data subject rights, DPO, DPIA, ROPA, breach response, international transfers, and more.

Published by
Compliance Enablers LLP

Last Updated
March 2026

Pages
~14 pages

Introduction

The General Data Protection Regulation (GDPR) is the European Union's comprehensive data protection law that came into effect on 25 May 2018. It applies to any organization that processes the personal data of individuals in the EU/EEA, regardless of where the organization is based. Non-compliance can result in fines of up to 20 million euros or 4% of annual global turnover, whichever is greater.

This checklist provides a structured, actionable guide to achieving and maintaining GDPR compliance. It is organized into ten key requirement areas, with specific items you can use to assess your readiness. Each item includes a brief explanation of what is needed and why.

Use this checklist as a self-assessment tool, an audit preparation guide, or a roadmap for building your GDPR compliance program.

1. Lawful Basis & Consent

Every processing activity must have a valid lawful basis under Article 6 of the GDPR. Where consent is used, it must meet strict requirements.

- [ ] **1.1 Identify lawful basis for each processing activity** Document which of the six lawful bases (consent, contract, legal obligation, vital interests, public task, legitimate interests) applies to each processing activity. Record this in your Records of Processing Activities.
- [ ] **1.2 Conduct Legitimate Interest Assessments (LIAs)** Where legitimate interests is the lawful basis, perform and document a balancing test that weighs your interests against the data subject's rights and freedoms. Keep LIAs on file for accountability.
- [ ] **1.3 Obtain consent using a compliant mechanism** Where consent is the lawful basis, ensure it is freely given, specific, informed, and unambiguous. Use clear affirmative action (opt-in, not pre-ticked boxes). Consent must be as easy to withdraw as to give.
- [ ] **1.4 Maintain consent records** Record who consented, when, how, what they were told at the time, and whether they have withdrawn consent. These records must be accessible for audit purposes.
- [ ] **1.5 Provide a clear mechanism to withdraw consent** Individuals must be able to withdraw consent at any time through an easy, accessible process. Upon withdrawal, cease the processing that relied on that consent.
- [ ] **1.6 Separate consent from other terms and conditions** Do not bundle consent for data processing with acceptance of terms of service. Consent must be granular and specific to each processing purpose.
- [ ] **1.7 Verify age for children's data** If you offer online services directly to children, implement age verification mechanisms and obtain parental/guardian consent where required. The age threshold varies by EU member state (13-16 years).
- [ ] **1.8 Review lawful basis regularly** Periodically reassess whether the lawful basis for each processing activity remains valid. Changes in processing purposes or data types may require a different basis.

2. Data Subject Rights

Under Articles 12-22, individuals have extensive rights over their personal data. You must have processes to handle these rights within the statutory timeframes.

- [ ] **2.1 Establish a process for handling data subject requests** Create a documented procedure for receiving, verifying, processing, and responding to data subject access requests (DSARs) and other rights requests. Designate responsible personnel.
- [ ] **2.2 Respond to requests within 30 days** The standard response time is one month from receipt. Extensions of up to two additional months are allowed for complex or numerous requests, but you must inform the individual within the first month.
- [ ] **2.3 Facilitate the right of access (Article 15)** Provide individuals with confirmation of whether their data is processed, a copy of the data, and supplementary information (purposes, categories, recipients, retention periods, rights, source, automated decision-making).
- [ ] **2.4 Facilitate the right to rectification (Article 16)** Correct inaccurate personal data without undue delay upon request. Complete incomplete data where appropriate.

- [ ] **2.5 Facilitate the right to erasure (Article 17)** Delete personal data upon request where the data is no longer necessary, consent is withdrawn, the individual objects and there are no overriding grounds, the data was unlawfully processed, or erasure is required by law.
- [ ] **2.6 Facilitate the right to restriction of processing (Article 18)** Restrict processing when the accuracy is contested, processing is unlawful but the individual opposes erasure, the data is no longer needed but required for legal claims, or the individual has objected pending verification of grounds.
- [ ] **2.7 Facilitate the right to data portability (Article 20)** Provide personal data in a structured, commonly used, machine-readable format when processing is based on consent or a contract and is carried out by automated means. Enable direct transmission to another controller where technically feasible.
- [ ] **2.8 Facilitate the right to object (Article 21)** Stop processing personal data for direct marketing immediately upon objection. For processing based on legitimate interests or public task, cease unless you demonstrate compelling legitimate grounds that override the individual's interests.
- [ ] **2.9 Address automated decision-making and profiling (Article 22)** Do not subject individuals to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects, unless based on explicit consent, contract necessity, or authorized by law. Provide the right to human intervention.
- [ ] **2.10 Verify identity before fulfilling requests** Implement reasonable identity verification procedures to ensure you are responding to the actual data subject. Do not request excessive information for verification purposes.

3. Privacy Notices & Transparency

Articles 13 and 14 require that individuals are clearly informed about how their data is collected and used.

- [ ] **3.1 Provide a privacy notice at the point of data collection** When collecting data directly from individuals, present a privacy notice at the time of collection. When obtaining data from third parties, provide the notice within a reasonable period (and no later than one month).
- [ ] **3.2 Include all required information in privacy notices** Your notice must include: controller identity and contact details, DPO contact details (if applicable), purposes and lawful basis, legitimate interests (if applicable), recipients/categories of recipients, international transfer details, retention periods, data subject rights, right to withdraw consent, right to complain to a supervisory authority, whether provision of data is statutory/contractual/obligatory, and information about automated decision-making.
- [ ] **3.3 Use clear, plain language** Privacy notices must be concise, transparent, intelligible, and easily accessible. Avoid legal jargon. Use layered notices where appropriate (short notice + detailed policy). Provide notices in the language of the target audience.
- [ ] **3.4 Maintain separate notices for different audiences** If you collect data from different groups (customers, employees, job applicants, website visitors), create tailored privacy notices for each audience reflecting their specific processing activities.
- [ ] **3.5 Keep privacy notices up to date** Review and update privacy notices whenever processing activities change. Inform individuals of significant changes to how their data is processed.
- [ ] **3.6 Make privacy notices easily accessible** Publish privacy notices prominently on your website, within your application, and at physical points of data collection. Ensure they are accessible to individuals with disabilities.

4. Data Protection Officer (DPO)

Articles 37-39 specify when a DPO must be appointed and define the role's responsibilities.

- [ ] **4.1 Determine if a DPO is required** A DPO is mandatory if you are a public authority, your core activities require regular and systematic monitoring of individuals on a large scale, or your core activities involve large-scale processing of special category data or data relating to criminal convictions. Even if not mandatory, consider appointing one voluntarily.
- [ ] **4.2 Appoint a qualified DPO** The DPO must have expert knowledge of data protection law and practices. The DPO can be an internal employee or external service provider. Ensure they have the resources and access needed to fulfill their duties.
- [ ] **4.3 Ensure DPO independence** The DPO must not receive instructions regarding the exercise of their tasks, must not be dismissed or penalized for performing their duties, and must report directly to the highest management level.
- [ ] **4.4 Publish DPO contact details** Make DPO contact details available to data subjects and communicate them to your supervisory authority. Include DPO contact information in your privacy notices.

- [ ] **4.5 Involve the DPO in all data protection matters** Ensure the DPO is consulted on Data Protection Impact Assessments, data breach responses, policy development, and any processing activity changes with data protection implications.

5. Data Protection Impact Assessment (DPIA)

Article 35 requires DPIAs for processing that is likely to result in a high risk to individuals' rights and freedoms.

- [ ] **5.1 Identify when a DPIA is required** A DPIA is mandatory for: systematic and extensive profiling with significant effects, large-scale processing of special category data, systematic monitoring of publicly accessible areas, and any processing on your supervisory authority's DPIA-required list.
- [ ] **5.2 Conduct DPIAs before processing begins** Perform the DPIA prior to commencing the processing activity, not after the fact. Build DPIA requirements into your project management and change management processes.
- [ ] **5.3 Include all required elements in the DPIA** Each DPIA must describe the processing operations and purposes, assess the necessity and proportionality, identify and assess risks to individuals, and describe measures to address those risks.
- [ ] **5.4 Consult with the DPO** Seek the DPO's advice when carrying out a DPIA. Document their input and any recommendations.
- [ ] **5.5 Consult the supervisory authority when required** If a DPIA reveals a high risk that cannot be mitigated, consult with your supervisory authority before proceeding with the processing.
- [ ] **5.6 Review and update DPIAs** Revisit DPIAs when there are changes to the processing, the technology, the context, or when new risks emerge. DPIAs are living documents.

6. Records of Processing Activities (ROPA)

Article 30 requires controllers and processors to maintain records of their processing activities.

- [ ] **6.1 Maintain a Register of Processing Activities** Document all processing activities including: name and contact details of the controller/processor, purposes of processing, categories of data subjects and personal data, categories of recipients, international transfers, retention periods, and a general description of technical and organizational security measures.
- [ ] **6.2 Include all processing activities** Cover all data processing — not just digital. Include paper records, CCTV, employee monitoring, marketing activities, HR processing, customer data, partner/vendor data, and website analytics.
- [ ] **6.3 Assign process owners** Each processing activity should have a designated owner responsible for maintaining accuracy and ensuring compliance.
- [ ] **6.4 Document the lawful basis for each activity** Record which of the six lawful bases applies to each processing activity in your ROPA.
- [ ] **6.5 Document data flows** Map where personal data flows — from collection through processing, storage, sharing, and deletion. Identify all systems, databases, and third parties involved.
- [ ] **6.6 Specify retention periods** Define and document how long personal data is retained for each processing activity. Ensure retention periods are justifiable and not longer than necessary.
- [ ] **6.7 Make records available to the supervisory authority** Be prepared to provide your ROPA to the supervisory authority upon request. Maintain it in a format that is easily accessible and understandable.
- [ ] **6.8 Review and update ROPA regularly** Review the ROPA at least annually and whenever processing activities change. Assign responsibility for keeping it current.

7. Data Breach Response

Articles 33 and 34 impose strict breach notification obligations with tight timelines.

- [ ] **7.1 Establish a data breach response procedure** Document a clear procedure covering: breach detection and identification, initial assessment and containment, risk assessment (impact on individuals), notification decision-making, internal escalation, external notification (supervisory authority and data subjects), and post-incident review.
- [ ] **7.2 Notify the supervisory authority within 72 hours** If a breach is likely to result in a risk to individuals' rights and freedoms, notify the relevant supervisory authority without undue delay and no later than 72 hours after becoming aware of it. If notification is delayed beyond 72 hours, provide reasons for the delay.

- [ ] **7.3 Notify affected individuals without undue delay** If a breach is likely to result in a high risk to individuals' rights and freedoms, notify the affected individuals directly. The notification must describe the breach, likely consequences, measures taken, and DPO/contact point details.
- [ ] **7.4 Maintain a breach register** Record all personal data breaches regardless of whether they are notifiable. Document the facts, effects, and remedial actions for each breach. This register demonstrates accountability to the supervisory authority.
- [ ] **7.5 Train staff on breach identification and reporting** Ensure all employees know how to recognize a potential data breach and how to report it internally. Include breach awareness in security awareness training programs.
- [ ] **7.6 Test breach response procedures** Conduct regular tabletop exercises or simulations to test your breach response procedure. Identify gaps and improve processes based on lessons learned.
- [ ] **7.7 Engage legal and communications teams** Ensure legal counsel and communications/PR teams are integrated into the breach response plan. Legal advice is critical for notification decisions, and communications teams manage public/customer messaging.

8. International Transfers

Chapter V (Articles 44-50) restricts transfers of personal data outside the EU/EEA unless adequate safeguards are in place.

- [ ] **8.1 Identify all international data transfers** Map all instances where personal data is transferred outside the EU/EEA, including cloud services, SaaS providers, group companies, outsourced services, and remote access by personnel in non-EU countries.
- [ ] **8.2 Verify the transfer mechanism** Ensure each transfer has a valid legal mechanism: adequacy decision (approved countries), Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), approved codes of conduct, approved certification mechanisms, or derogations (explicit consent, contract necessity, etc.).
- [ ] **8.3 Conduct Transfer Impact Assessments (TIAs)** When relying on SCCs or BCRs, assess whether the laws of the recipient country provide adequate protection for personal data. Document your assessment and any supplementary measures needed.
- [ ] **8.4 Implement supplementary measures where necessary** If the TIA reveals that the transfer mechanism alone is insufficient, implement supplementary technical (encryption, pseudonymization), organizational (access restrictions, policies), or contractual measures.
- [ ] **8.5 Monitor changes in adequacy decisions and transfer mechanisms** Stay current on European Commission adequacy decisions, court rulings (such as Schrems II and its successors), and regulatory guidance that may affect your transfer mechanisms.

9. Vendor / Processor Management

Article 28 imposes specific obligations on controllers when engaging processors (vendors who process personal data on your behalf).

- [ ] **9.1 Identify all processors** Maintain an inventory of all third parties that process personal data on your behalf, including cloud providers, SaaS platforms, payroll providers, marketing platforms, analytics tools, customer support tools, and IT managed service providers.
- [ ] **9.2 Conduct due diligence before engaging processors** Before engaging a processor, verify that they provide sufficient guarantees regarding GDPR compliance, security measures, and data protection capabilities. Review their certifications, audit reports (SOC 2, ISO 27001), and privacy policies.
- [ ] **9.3 Execute a Data Processing Agreement (DPA)** A written agreement with each processor is mandatory. The DPA must include: subject matter and duration, nature and purpose of processing, types of personal data and data subjects, controller's obligations and rights, processor's obligations (including security measures, sub-processor management, breach notification, data return/deletion, audit rights).
- [ ] **9.4 Manage sub-processors** Require processors to obtain your authorization before engaging sub-processors. Maintain visibility into the sub-processor chain. Ensure equivalent contractual obligations flow down.
- [ ] **9.5 Audit processors periodically** Exercise your audit rights to verify processor compliance. This can include on-site audits, reviewing independent audit reports, or sending security questionnaires. Frequency should be risk-based.
- [ ] **9.6 Ensure processor breach notification obligations** Your DPA must require processors to notify you without undue delay upon becoming aware of a personal data breach. Define specific timelines (e.g., within 24 hours) and

information requirements.

10. Technical & Organizational Measures

Article 32 requires appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

- [ ] **10.1 Implement access controls** Apply the principle of least privilege. Use role-based access control (RBAC), require multi-factor authentication (MFA) for all systems containing personal data, conduct regular access reviews, and implement strong password policies.
- [ ] **10.2 Encrypt personal data** Implement encryption for data in transit (TLS 1.2+) and at rest (AES-256). Apply encryption to databases, backups, portable devices, and email communications containing personal data.
- [ ] **10.3 Implement pseudonymization where appropriate** Use pseudonymization techniques (tokenization, key-coded data) to reduce the risks of processing. Pseudonymized data is still personal data under GDPR, but it reduces impact in the event of unauthorized access.
- [ ] **10.4 Ensure data integrity and availability** Implement regular backups, test restoration procedures, deploy redundant systems for critical processing, and establish business continuity and disaster recovery plans.
- [ ] **10.5 Implement logging and monitoring** Log access to systems containing personal data, monitor for unauthorized access or anomalous activity, retain logs for an appropriate period, and protect log integrity against tampering.
- [ ] **10.6 Apply data minimization in practice** Collect only the personal data that is necessary for the specified purpose. Review data collection forms, APIs, and processes to eliminate unnecessary data fields. Implement automated data deletion when retention periods expire.
- [ ] **10.7 Conduct regular security testing** Perform vulnerability assessments, penetration testing, and security code reviews on systems that process personal data. Address identified vulnerabilities according to risk severity and within defined timelines.
- [ ] **10.8 Maintain a security awareness training program** Train all employees who handle personal data on GDPR requirements, data handling procedures, breach identification and reporting, and secure computing practices. Deliver training at onboarding and at regular intervals thereafter.

Summary: Compliance at a Glance

Requirement Area	Items	Status
Lawful Basis & Consent	8 items	__ / 8 complete
Data Subject Rights	10 items	__ / 10 complete
Privacy Notices & Transparency	6 items	__ / 6 complete
Data Protection Officer	5 items	__ / 5 complete
Data Protection Impact Assessment	6 items	__ / 6 complete
Records of Processing Activities	8 items	__ / 8 complete
Data Breach Response	7 items	__ / 7 complete
International Transfers	5 items	__ / 5 complete
Vendor/Processor Management	6 items	__ / 6 complete
Technical & Organizational Measures	8 items	__ / 8 complete
Total	69 items	__ / 69 complete

Next Steps

1. **Assess your current state**: Work through this checklist, marking items as complete, in progress, or not started.
2. **Prioritize gaps**: Focus first on high-risk areas — breach response, lawful basis, and data subject rights processes.

3. **Assign ownership**: Designate responsible individuals for each requirement area.
4. **Set deadlines**: Create a remediation timeline with realistic milestones.
5. **Document everything**: GDPR's accountability principle (Article 5(2)) requires you to demonstrate compliance, not just achieve it.
6. **Review regularly**: Compliance is not a one-time exercise. Review this checklist quarterly and after any significant changes to your processing activities.

This resource is provided by Compliance Enablers — the unified GRC platform with 27 modules, 261+ compliance frameworks, and built-in security awareness training. Learn more at complianceenablers.com

Ready to Transform Your Compliance Program?

27 modules • 261+ frameworks • 157 templates • 40+ integrations • AI-powered • From $999/yr

Schedule a Demo | Start Free Trial