AUGMENTIVE BUSINESS 7 SOLUTIONS PVT. LTD.

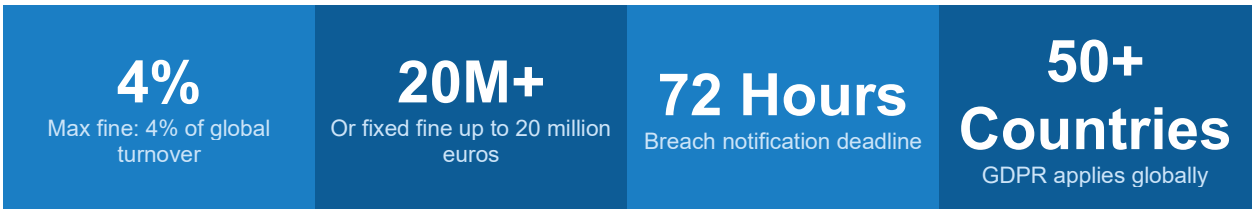
COMPLIANCE CHECKLISTS

Data Protection & GDPR Compliance for Outsourcing

Essential compliance requirements for handling EU customer data with remote teams. Includes Data Processing Agreements.

Executive Summary

If your company handles personal data of individuals in the European Union, GDPR (General Data Protection Regulation) applies regardless of where your company is located. This comprehensive guide covers GDPR fundamentals, the 7 data protection principles, 6 lawful bases for processing, data subject rights, Data Processing Agreements (DPAs), Standard Contractual Clauses (SCCs), security requirements, breach notification procedures, and India DPDP Act 2023 compliance for offshore teams.



GDPR Fundamentals

What Is GDPR?

The General Data Protection Regulation (GDPR, EU Regulation 2016/679) is the European Union's comprehensive data protection law that governs how organizations collect, process, store, and use personal data of individuals in the EU. It applies globally: any company that processes personal data of EU residents must comply, regardless of where the company is located.

Key Definitions:

- Personal Data: Any information relating to an identified or identifiable natural person (name, email, IP address, ID number, biometric data, location data, etc.)
- Processing: Any operation performed on personal data (collection, recording, organization, use, transfer, deletion, etc.)
- Data Controller: Organization that determines the purpose and means of processing (typically your company)
- Data Processor: Organization that processes data on behalf of the controller (e.g., hosting provider, CRM vendor)
- Data Subject: The individual to whom the personal data belongs

Scope of GDPR:

GDPR applies if:

- You process personal data of EU residents, AND
- Your company is established in the EU, OR
- You offer goods/services to EU residents, OR
- You monitor EU residents' behavior online

Penalties for Non-Compliance:

- Administrative fine up to 20 million euros or 4% of global annual revenue (whichever is higher) for serious violations
- Fine up to 10 million euros or 2% of global revenue for lesser violations
- Individual liability for executives and employees
- Private lawsuits from individuals claiming damages

Key Concept: Lawful Basis

You cannot process personal data without a lawful legal basis. This is the foundation of GDPR compliance. We will explore the 6 lawful bases in detail below.

GDPR 7 Data Protection Principles

All personal data processing must comply with these 7 principles. Use this checklist to verify your company's compliance:

- ✓ 1. Lawfulness, Fairness, Transparency: Data is processed lawfully, fairly, and transparently. You must have a lawful basis. Processing must not be deceptive.
- ✓ 2. Purpose Limitation: Data is collected for specific, explicit, legitimate purposes. Cannot be repurposed without consent.
- ✓ 3. Data Minimization: Only collect data necessary for the stated purpose. Do not over-collect.
- ✓ 4. Accuracy: Data must be accurate and up-to-date. Implement processes to correct inaccurate data.
- ✓ 5. Storage Limitation: Data is kept only as long as necessary. Implement data retention schedules and deletion procedures.
- ✓ 6. Integrity and Confidentiality: Data is secure against unauthorized access, alteration, or loss. Implement technical and organizational safeguards.
- ✓ 7. Accountability: You must demonstrate compliance. Document all processing activities and maintain records.

Accountability Documentation:

To demonstrate compliance (Principle 7), maintain:

- Data Processing Impact Assessment (DPIA) for high-risk processing
- Data Processing Agreement with processors
- Data Retention Schedule
- Employee training records
- Breach incident logs and investigation reports

6 Lawful Bases for Processing

You must have at least ONE lawful basis to process personal data. Here are the 6 bases and examples:

Basis	Definition	When to Use	Example
Consent	Data subject explicitly agrees to processing	Marketing, non-essential processing, cookies	Newsletter signup form with explicit checkbox
Contract	Processing necessary to perform contract with data subject	Customer order fulfillment, employee records	Processing payment info to deliver purchased product
Legal Obligation	Processing required by law	Tax records, employment records, regulatory compliance	Tax authority requires employee records for 10 years
Vital Interests	Processing necessary to protect vital interests (life or health)	Emergency response, medical services	Hospital processing unconscious patient's data to provide care
Public Task	Processing necessary for public authority performing public function	Government agencies, public services	Ministry processing citizen data for social services
Legitimate Interests	Pursues legitimate business interest that does not override data subject rights	Fraud detection, direct marketing, analytics	Company analyzes customer behavior to prevent fraud

Lawful Basis Analysis:

For each data processing activity, document:

1. Which lawful basis applies
2. Why processing is necessary
3. How it benefits your business or complies with law
4. Risks to data subjects

Example (E-commerce Company):

- Activity: Process customer email address for order confirmation
- Lawful basis: Contract (necessary to fulfill purchase)
- Documentation: Processing is essential to email order details and shipping status

Special Handling: Sensitive Data

Processing sensitive personal data (ethnicity, religion, health, biometric, sexual orientation) is generally prohibited UNLESS:

- Explicit consent is obtained, OR
- Processing is necessary for employment/social security law, OR
- Data subject has publicly disclosed the data, OR
- Necessary for vital interests, OR

- Necessary for legal claims

Most companies should never process sensitive data without explicit consent.

8 Data Subject Rights (Checklist)

Data subjects (individuals) have the following rights. Your company must honor these requests within 30 days (or 90 days if complex):

Right	Definition	Example	How to Respond
Access (Art. 15)	Individual can request copy of all personal data you hold	"Send me all data you have on me"	Provide free copy of all personal data within 30 days; common format: CSV or PDF
Rectification (Art. 16)	Individual can correct inaccurate data	"My phone number is wrong; fix it"	Correct the data and notify all processors who received it
Erasure (Art. 17)	"Right to be forgotten" — request deletion of data	"Delete my account and all my data"	Delete data unless exception applies (e.g., legal obligation, exercise of rights)
Restrict Processing (Art. 18)	Individual can pause processing while disputing accuracy or request	"Keep my data but stop using it"	Stop all processing except storage until dispute resolved
Portability (Art. 20)	Individual can receive data in structured, portable format for transfer to another service	"I want my data in Excel to move to competitor"	Provide data in machine-readable format (CSV, JSON, XML) at no cost
Withdraw Consent (Art. 7)	If processing is based on consent, individual can withdraw consent	"Unsubscribe from emails"	Stop processing immediately; no penalty
Object (Art. 21)	Individual can object to processing based on legitimate interests or direct marketing	"Stop profiling me for ads"	Stop processing (if legitimate interest or direct marketing); if other basis, respond to why processing continues
Automated Decisions (Art. 22)	Individual has right not to be subject to automated decision-making that produces legal effect	"Don't use AI to deny my loan"	Do not use automated decisions for consequential determinations without human review

Handling Data Subject Requests:

5. Verify identity of requester (must confirm they are the data subject)
6. Create request log with date, subject, deadline
7. Conduct internal data search to identify all personal data

8. Compile and respond within 30 days (or 90 days if complex)
9. Document all steps and maintain records

Costs:

Most requests must be honored at no cost to the individual. You can only charge if requests are repetitive or manifestly unfounded.

> **Best Practice**
> Data subject rights are frequently tested. Build a system to handle requests quickly. Delays or refusals can trigger regulatory fines and lawsuits. Aim to respond within 14 days to build goodwill.

Controller vs. Processor: Legal Relationship Table

Understanding your role is critical to GDPR obligations:

Role	Definition	Who Decides?	Responsibilities	Liability
Data Controller	Determines PURPOSE and MEANS of processing	Controller decides what to collect and why	Determine lawful basis; ensure data quality; honor subject rights; security safeguards	Directly liable to data subjects; fined up to 4% revenue
Data Processor	Processes data ON BEHALF of controller; does not determine purpose/means	Controller determines; processor implements	Implement safeguards per contract; assist controller with subject rights; report breaches	Liable for security failures; fined up to 2% revenue
Joint Controllers	Two or more entities decide PURPOSE and MEANS together	Shared decision-making	Share responsibility; establish which entity is responsible for which obligation	Both entities jointly liable; can sue each other
Sub-Processor	Processor hires another processor to assist (e.g., cloud host using another host)	Processor authorizes; controller approves	Same as processor; ensure sub-processor complies	Processor liable for sub-processor failures

Your Company's Likely Role:

If your company collects customer data directly (even through a vendor), you are likely the CONTROLLER. Your vendors (CRM, email platform, hosting) are PROCESSORS.

Controller Obligations:

- Determine lawful basis for all processing
- Conduct Data Protection Impact Assessment (DPIA) for high-risk processing
- Publish Privacy Policy
- Sign Data Processing Agreement with all processors
- Respond to data subject rights requests
- Report data breaches to regulators within 72 hours
- Maintain processing documentation

Processor Obligations:

- Sign Data Processing Agreement with controller
- Implement technical and organizational security measures
- Not use data for own purposes
- Report any breach to controller within 24 hours
- Assist controller with subject rights requests
- Maintain processing documentation

Data Processing Agreement (DPA) Requirements

You must have a signed Data Processing Agreement with every processor (vendor) who handles personal data. The DPA must include:

Essential DPA Clauses (Checklist):

- ✓ Subject matter and duration of processing
- ✓ Nature and purpose of processing
- ✓ Types of personal data processed
- ✓ Categories of data subjects
- ✓ Rights and obligations of controller
- ✓ Rights and obligations of processor
- ✓ Processor must process only on instructions from controller
- ✓ Processor must ensure persons authorized to process data are under confidentiality obligations
- ✓ Processor implements appropriate security measures (encryption, access controls, etc.)
- ✓ Processor must report data breach to controller within 24 hours
- ✓ Processor must assist controller in responding to subject rights requests
- ✓ Processor may not engage sub-processors without prior written authorization from controller
- ✓ Controller may audit processor's security measures
- ✓ Processor must delete or return data when contract ends
- ✓ Processor must assist controller with Data Protection Impact Assessment (DPIA)

Where to Find Standard DPA:

Most SaaS vendors (Google, Microsoft, Salesforce, Slack, etc.) have pre-made DPA templates. Request their standard DPA before signing service agreement.

Red Flag:

If a vendor refuses to sign a DPA or will not commit to GDPR compliance, DO NOT use them for processing EU personal data. This is a compliance violation.

Standard Contractual Clauses (SCCs) for International Data Transfers

The Problem: Data Localization

GDPR generally requires personal data to remain in the EU. If you transfer data to countries outside the EU (USA, India, etc.), you must have a legal mechanism. In 2020, the EU struck down the Privacy Shield agreement, making data transfers to the US legally risky.

Solution: Standard Contractual Clauses (SCCs)

SCCs are pre-approved EU contract templates that allow data transfers outside the EU. They include contractual guarantees that the recipient will protect data as if in the EU.

When Do You Need SCCs?

You need SCCs if:

- You transfer personal data to a processor outside the EU
- You have employees or contractors in non-EU countries accessing EU personal data
- You use cloud hosting outside the EU
- You use US-based SaaS tools (Google, Microsoft, Salesforce, etc.)

SCC Options:

- Module One (Controller to Processor): Use when your processor is outside EU
- Module Two (Controller to Controller): Use when data is shared with another company outside EU
- Module Three (Processor to Sub-processor): Use when processor hires sub-processor outside EU
- Module Four (Processor to Controller): Use when processor transfers data to controller outside EU

Practical Implementation:

Most SaaS vendors have already signed EU-approved SCCs and included them in their DPA. Verify this in writing before using the vendor.

Supplementary Measures:

After Schrems II ruling (July 2020), SCCs alone may not be sufficient. You must also implement supplementary measures:

- Encryption of data in transit and at rest
- Access controls limiting who can view data
- Pseudonymization (replacing identifiers with coded values)
- Contractual commitments not to disclose to government unless legally required

> **Transfer Risk**
> Data transfers are the most complex aspect of GDPR for international companies. If in doubt, consult a GDPR lawyer on your specific data transfer arrangements.

Security Requirements Checklist (20+ Items)

GDPR requires appropriate technical and organizational measures to protect personal data security. Here is a comprehensive checklist:

Access Control:

- ✓ Implement role-based access control (RBAC) — users only access data needed for their role
- ✓ Use unique user IDs (no shared logins)
- ✓ Enable multi-factor authentication (MFA) for all accounts
- ✓ Implement password policies: minimum 12 characters, changed quarterly
- ✓ Maintain access logs of who accessed what data and when
- ✓ Conduct quarterly access reviews and revoke unused accounts
- ✓ Restrict access to sensitive data to small number of people
- ✓ Require managers to approve all access requests

Encryption:

- ✓ Encrypt all personal data in transit (TLS 1.2 or higher)
- ✓ Encrypt all personal data at rest (AES-256 or equivalent)
- ✓ Manage encryption keys securely (never hardcode keys in code)
- ✓ Rotate encryption keys annually
- ✓ Use separate encryption keys for different environments (prod vs dev)
- ✓ Ensure encrypted backups are also secured

Data Management:

- ✓ Implement data retention schedule (delete data after specified period)
- ✓ Pseudonymize data where possible (replace identifiers with coded values)
- ✓ Delete data that is no longer needed
- ✓ Maintain secure data disposal procedures (cannot simply delete files)
- ✓ Segment data by sensitivity; store sensitive data separately
- ✓ Limit data transfers between systems; use APIs instead of file exports

Infrastructure Security:

- ✓ Use reputable, compliant hosting providers (AWS, Azure, Google Cloud with GDPR compliance)
- ✓ Implement firewall and intrusion detection systems
- ✓ Conduct vulnerability assessments quarterly
- ✓ Apply security patches within 30 days of release
- ✓ Disable unnecessary services and ports
- ✓ Implement network segmentation (separate networks for sensitive data)

- ✓ Monitor network traffic for anomalies

Endpoint Security:

- ✓ Install and maintain antivirus on all devices
- ✓ Enable automatic OS and software updates
- ✓ Require full disk encryption on laptops and mobile devices
- ✓ Enable remote wipe capability for lost devices
- ✓ Block USB ports on company computers
- ✓ Disable personal device connections unless authorized
- ✓ Require VPN for remote access

Incident Response:

- ✓ Implement incident response plan with clear escalation procedures
- ✓ Designate data breach response team
- ✓ Maintain breach notification templates
- ✓ Conduct tabletop exercises annually to test response
- ✓ Log all security incidents for investigation
- ✓ Report breaches to regulators within 72 hours
- ✓ Notify affected individuals if high risk

Personnel Security:

- ✓ Conduct background checks on employees handling personal data
- ✓ Require GDPR training for all staff
- ✓ Require confidentiality agreements (NDAs)
- ✓ Implement access restrictions based on role
- ✓ Conduct security awareness training quarterly
- ✓ Test staff with simulated phishing emails
- ✓ Have incident reporting procedure staff know about

Vendor Management:

- ✓ Audit processors' security measures before engagement
- ✓ Require signed Data Processing Agreement (DPA)
- ✓ Conduct annual security assessments of processors
- ✓ Require processors to notify you of data breaches immediately
- ✓ Restrict processors from using sub-processors without approval
- ✓ Maintain list of all processors and their sub-processors

Data Protection Impact Assessment (DPIA)

When Is a DPIA Required?

You must conduct a DPIA for high-risk processing. High-risk includes:

- Large-scale processing of personal data
- Systematic monitoring of behavior (tracking, profiling)
- Processing of sensitive data (health, biometric, criminal)
- Automated decision-making with legal effects
- Use of new technologies

If you use standard CRM, email, or analytics tools, you likely still need a DPIA.

DPIA Content:

10. Describe processing activity and legitimate interest
11. Assess necessity and proportionality of processing
12. Analyze risks to data subjects
13. Describe mitigation measures
14. Consult with privacy officer and key stakeholders
15. Document findings and store for regulator review

DPIA Template Topics:

- Processing activity name and description
- Legal basis for processing
- Data types and volume
- Data subjects affected
- System description and controls
- Risk assessment (likelihood and impact)
- Mitigation measures

72-Hour Breach Notification Protocol

What Constitutes a Data Breach?

A breach is any unauthorized access, alteration, loss, or disclosure of personal data. This includes:

- Hacking or unauthorized access
- Malware or ransomware infection
- Accidental disclosure (email to wrong recipient, unencrypted file)
- Lost or stolen device
- Insider theft

72-Hour Notification Rule:

If a breach compromises personal data, you must notify regulators (Data Protection Authority) within 72 hours of discovering the breach. If data poses high risk to individuals, you must also notify individuals directly.

Step-by-Step Breach Protocol:

16. Discovery (0 hours): Breach is detected or reported
17. Initial Response (0-4 hours): Isolate affected systems, stop ongoing compromise, preserve evidence
18. Investigation (4-24 hours): Determine scope, data affected, individuals impacted, cause
19. Notification Prep (24-48 hours): Prepare regulatory notification and individual notices
20. Regulatory Notification (48-72 hours): Notify Data Protection Authority
21. Individual Notification (Same day or day after): Notify affected individuals of breach
22. Documentation (Within 30 days): Complete incident report and add to breach log

Breach Notification Content:

Notification to regulators must include:

- Name and contact of controller
- Description of breach (what happened)
- Likely consequences for data subjects
- Measures taken or proposed to address breach
- Contact for more information

Individual Notification:

Tell affected individuals:

- What personal data was breached
- What happened (in plain language)
- Likely consequences for them
- What you are doing to fix it
- Who to contact with questions

Use simple, non-technical language. Avoid legal jargon.

Exceptions (No Individual Notification Required):

You do NOT have to notify individuals if:

- Data was encrypted and encryption was not compromised
- Risk is low (data unlikely to cause harm)
- You implement safeguards quickly (e.g., individual still does not face risk)

> **Detection Matters**
> The 72-hour clock starts when you DISCOVER the breach, not when it occurred. If you don't monitor systems well, discovery is delayed and notification clock starts late. Invest in breach detection tools (SIEM, log monitoring, DLP).

India Data Protection Act 2023 (DPDP) Overview

India passed the Digital Personal Data Protection Act, 2023 (DPDP), similar in scope to GDPR. If you hire remote workers in India who access personal data, they must comply with DPDP.

Key DPDP Provisions:

- Consent required for all personal data processing (similar to GDPR)
- Data fiduciary (processor) must implement reasonable safeguards
- Data localization: Sensitive data must be stored in India
- Rights: Individuals can correct, erasure, portability requests
- Data Protection Board enforces DPDP (government body)
- Penalties up to 5 crore rupees (~$600,000 USD) for serious violations

Practical Implications for Offshore Teams:

If hiring Indian contractors to process EU customer data:

- Data must comply with both GDPR (EU) and DPDP (India)
- Indian contractor must sign DPDP-compliant processing agreement
- Personal data must be encrypted in transit and at rest
- Indian data must not be transferred out of India except to approved countries
- Your company bears responsibility for contractor's DPDP compliance

Alignment with GDPR:

DPDP is largely compatible with GDPR, but has some differences:

- DPDP is less prescriptive on security measures (GDPR details requirements more)
- DPDP does not prohibit sensitive data processing if explicit consent (GDPR is stricter)
- DPDP has data localization requirement (GDPR does not)

Best Practice:

Treat DPDP requirements as equal to GDPR. If your data processing satisfies GDPR, it likely satisfies DPDP. Document compliance with both.

Privacy Policy Requirements

You must publish a Privacy Policy on your website that explains your data processing. Privacy Policy must include:

Required Sections:

- Contact information (name, email, address of controller and data protection officer)
- Processing purposes (what data you collect and why)
- Data categories (email, name, phone, IP address, etc.)
- Lawful basis (consent, contract, legitimate interest, etc.)
- Recipients (who you share data with)
- Data subject rights (access, erasure, portability, etc.)
- Retention period (how long you keep data)
- Data sources (where you get data from)
- Cookies and tracking technologies (if applicable)
- Third-party services (Google Analytics, email providers, etc.)
- International transfers (if data goes to non-EU countries)
- Automated decision-making (if you use profiling or AI)
- Complaints procedure (how to file complaint with regulator)

Plain Language Requirement:

Privacy Policy must be in clear, plain language. Avoid legal jargon. Use short sentences and paragraphs. Mobile-friendly format recommended.

Cookie Notice:

If your website uses cookies, you must display a banner at first visit asking consent before setting cookies. Consent must be opt-in (not opt-out).

Do Not Bury Policy:

Privacy Policy must be easily accessible (link in footer, prominent location). Buried policies are not considered compliant.

GDPR Compliance Checklist (30+ Items)

Use this comprehensive checklist to verify your organization's GDPR compliance:

Governance & Documentation:

- ✓ Identify all personal data processing activities in your organization
- ✓ Document lawful basis for each processing activity
- ✓ Maintain Records of Processing (list of all processing activities)
- ✓ Create and publish Privacy Policy
- ✓ Conduct Data Protection Impact Assessment (DPIA) for high-risk processing
- ✓ Designate a Data Protection Officer (if required by regulation or operating at scale)
- ✓ Appoint Privacy Champion or Compliance Officer
- ✓ Establish Data Governance Committee
- ✓ Document all vendor relationships and processing arrangements
- ✓ Maintain evidence of compliance for regulator review

Legal Agreements:

- ✓ Sign Data Processing Agreement (DPA) with all processors
- ✓ Verify all processors have signed DPA
- ✓ Implement Standard Contractual Clauses (SCCs) for non-EU transfers
- ✓ Obtain commitment from processors on GDPR compliance
- ✓ Review vendor security certifications (SOC 2, ISO 27001, etc.)
- ✓ Include GDPR terms in all processor contracts
- ✓ Maintain current list of all sub-processors
- ✓ Obtain Data Protection Officer contact information from key processors

Data Minimization & Purpose Limitation:

- ✓ Review data collection forms — remove unnecessary fields
- ✓ Implement data retention schedule (delete data when no longer needed)
- ✓ Delete old data at regular intervals (quarterly or annually)
- ✓ Stop collecting data when purpose is fulfilled
- ✓ Do not use data for secondary purposes without new consent
- ✓ Implement pseudonymization where possible (replace identifiers with codes)
- ✓ Segment sensitive data and apply stronger controls
- ✓ Maintain log of what data is collected, when, and from whom

Data Subject Rights:

- ✓ Establish process to respond to data access requests (30-day target)
- ✓ Implement system to track data subject requests
- ✓ Train staff on data subject rights

- ✓ Create email address for privacy requests (privacy@company.com)
- ✓ Respond to deletion requests within 30 days
- ✓ Respond to correction requests within 30 days
- ✓ Provide data in machine-readable format for portability requests
- ✓ Document all responses and maintain records

Security:

- ✓ Implement role-based access control (RBAC) for all data systems
- ✓ Enable multi-factor authentication (MFA) for all accounts
- ✓ Enable automatic screen locks after 15 minutes inactivity
- ✓ Encrypt all personal data in transit (TLS 1.2+)
- ✓ Encrypt all personal data at rest (AES-256 or equivalent)
- ✓ Conduct vulnerability assessment quarterly
- ✓ Apply security patches within 30 days of release
- ✓ Maintain security incident log
- ✓ Conduct annual security audit
- ✓ Implement backup and disaster recovery procedure
- ✓ Disable unnecessary services and ports on servers
- ✓ Monitor access logs for suspicious activity

Staff Training & Accountability:

- ✓ Require GDPR training for all staff at hire
- ✓ Conduct annual GDPR refresher training
- ✓ Test staff knowledge with quiz
- ✓ Maintain training attendance records
- ✓ Require confidentiality agreements (NDAs) from all employees
- ✓ Communicate privacy and security policies to all staff
- ✓ Establish incident reporting procedure
- ✓ Conduct tabletop breach response exercise annually

Breach Response:

- ✓ Create incident response plan with clear escalation
- ✓ Designate breach response team
- ✓ Maintain 72-hour breach notification procedure
- ✓ Prepare breach notification template
- ✓ Identify Data Protection Authority contact for your jurisdiction
- ✓ Maintain log of all security incidents
- ✓ Conduct root cause analysis for every incident

- ✓ Implement corrective actions within 30 days of incident

Vendor Management:

- ✓ Request signed DPA from all processors before engagement
- ✓ Conduct vendor security assessment before onboarding
- ✓ Verify vendor compliance certifications (SOC 2, ISO, etc.)
- ✓ Audit processors annually
- ✓ Request evidence of compliance from processors
- ✓ Maintain current list of all vendors and their sub-processors
- ✓ Ensure vendor is approved for non-EU data transfers (SCC, Privacy Shield, etc.)
- ✓ Have right to audit vendors in contract

Consent Management (If Using Consent Basis):

- ✓ Ensure consent is freely given, specific, informed, and unambiguous
- ✓ Use opt-in (not pre-checked boxes)
- ✓ Document when and how consent was obtained
- ✓ Maintain audit trail of consents
- ✓ Make it easy to withdraw consent
- ✓ Re-obtain consent every 2 years if data is old
- ✓ Separate consents for different processing purposes

GDPR Penalties Reference Table

Understanding potential penalties motivates compliance investment:

Violation Type	Severity	Fine Range	Examples	Annual Cap
Procedural violations (processing without basis, no DPA, no Privacy Policy)	Lesser	Up to 10M euros or 2% global revenue	No Data Processing Agreement; no Privacy Policy published	2% global annual revenue (20M euro max)
Security/technical violations (inadequate encryption, no access controls, no breach plan)	Lesser	Up to 10M euros or 2% global revenue	Data not encrypted; weak password policy; no breach response plan	2% global annual revenue (20M euro max)
Data subject rights violations (refusing access, delay, no records, ignoring requests)	Lesser	Up to 10M euros or 2% global revenue	Refuse to provide data access within 30 days; ignore deletion request	2% global annual revenue (20M euro max)
Core principle violations (no lawful basis, inadequate consent, unauthorized transfers)	Serious	Up to 20M euros or 4% global revenue	Process data without consent; transfer to non-approved country without SCC	4% global annual revenue (20M euro max)
Intentional violations (deliberately ignoring GDPR)	Serious	Up to 20M euros or 4% global revenue	Knowingly transfer data illegally; ignore regulator orders	4% global annual revenue (20M euro max)

Example Penalties (Real Cases):

- Google (2019): 50 million euros for lack of valid consent on cookies
- Amazon (2021): 746 million euros for insufficient legal basis and transparency
- Microsoft (2022): 60 million euros for unauthorized tracking via cookies

Individual Liability:

In addition to company fines, individuals (executives, managers) can be personally fined for GDPR violations. Maximum individual fine is 2 million euros or 40% of employee annual salary (whichever is higher).

Cost of Non-Compliance:

Typical company remediation costs $500K-$2M+ depending on breach size and complexity. Proactive compliance investment (documentation, training, tools) costs 5-10% of IT budget but prevents catastrophic penalties.

GDPR Action Plan: 90-Day Rollout

If you have not yet implemented GDPR compliance, use this 90-day plan:

Month 1: Assessment & Foundation

- ✓ Audit all data processing activities (interviews with departments)
- ✓ Identify all personal data systems and databases
- ✓ List all vendors/processors accessing personal data
- ✓ Request signed DPA from all vendors (non-negotiable)
- ✓ Designate Data Protection Officer or Privacy Champion
- ✓ Conduct gap assessment against 7 principles and 8 rights
- ✓ Schedule legal review of compliance status

Month 2: Documentation & Policies

- ✓ Create Records of Processing (document all processing activities)
- ✓ Conduct DPIA for high-risk processing
- ✓ Draft/update Privacy Policy
- ✓ Create breach response plan and incident templates
- ✓ Implement Data Processing Agreement template
- ✓ Standardize vendor contracts with GDPR terms
- ✓ Create data retention schedule
- ✓ Establish vendor audit checklist

Month 3: Technical Implementation & Training

- ✓ Implement encryption (in transit and at rest)
- ✓ Enable multi-factor authentication
- ✓ Set up access logging and monitoring
- ✓ Implement data deletion procedure
- ✓ Train all staff on GDPR and privacy
- ✓ Set up incident reporting email address
- ✓ Create data subject rights request process
- ✓ Conduct compliance audit and document readiness

Ongoing (After Month 3):

- ✓ Audit vendors annually
- ✓ Review data retention and delete old data quarterly
- ✓ Conduct staff training updates annually
- ✓ Test breach response procedures semi-annually
- ✓ Review and update Privacy Policy annually
- ✓ Monitor regulatory updates and adjust as needed

✓ Maintain comprehensive compliance documentation

Key GDPR vs. CCPA Differences (For US Companies)

If you operate in both EU and California:

Aspect	GDPR (EU)	CCPA (California)
Scope	All personal data of EU residents worldwide	Personal data of California residents doing business with CA companies
Penalties	Up to 4% global revenue	Up to $7,500 per intentional violation
Lawful Basis	Must have one of 6 lawful bases	Opt-out model (can use data unless consumer objects)
Consent	Opt-in (affirmative consent required)	Opt-out for most uses (CPRA makes some opt-in)
Rights	Access, Delete, Correct, Restrict, Portability, Object, Automated decisions	Access, Delete, Opt-out, Know what data is sold, Limit Use
Right to Erasure	Yes (Right to be Forgotten)	Yes (Right to Delete)
Data Minimization	Yes (collect only necessary)	No specific requirement
Privacy Officer	Required at scale	Not required

Practical Approach:

Most compliance experts recommend treating CCPA as the minimum standard and GDPR as the maximum. If you comply with GDPR, CCPA compliance is easier.

Resources & References

Official Guidance:

- EU GDPR Official Text: eur-lex.europa.eu
- European Data Protection Board (EDPB): edpb.ec.europa.eu
- Your Country Data Protection Authority (DPA)

Popular Tools:

- Consent Management Platforms: OneTrust, TrustArc, Cookiebot
- DPA Generators: TrustArc, EY, Deloitte templates
- Privacy Monitoring: GDPR Compliance Check
- Incident Management: Splunk, Rapid7, CrowdStrike

Recommended Consultants:

- Hire GDPR lawyer for Data Processing Agreement review
- Engage security firm for annual compliance audit
- Consider Data Protection Officer service (DPO outsourcing)

Training:

- Udemy GDPR courses
- CompTIA Security+ includes GDPR basics
- Coursera Introduction to GDPR

About AB7 Solutions
AB7 Solutions processes personal data for EU and global customers with full GDPR and DPDP compliance. Our Indian team is trained on GDPR, works under signed DPAs with SCCs, and maintains encryption and access controls per EU standards. All staff signs confidentiality agreements. Contact us for GDPR-compliant outsourcing.