



# Compliance And Data Privacy Checks

We are helping organizations ensure **compliance** and **data privacy** through structured, expert-led assessments and testing services. Here's how we typically support these areas:

---

## 1. Regulatory Compliance Testing

Testing consultancies can help ensure your software systems comply with industry-specific regulations such as:

- **GDPR** (General Data Protection Regulation)
- **HIPAA** (Health Insurance Portability and Accountability Act)
- **PCI-DSS** (Payment Card Industry Data Security Standard)
- **ISO/IEC 27001** (Information Security Management)

### What we do:

- Review policies and procedures for regulatory gaps
  - Validate that **data collection, processing, and storage** align with regulatory requirements
  - Simulate compliance audits
  - Map data flows and identify areas of risk or non-conformity
- 

## 2. Data Privacy & Security Testing

We perform technical and procedural checks to make sure personal and sensitive data is handled correctly.

### Common services:

- **Vulnerability assessments**
- **Penetration testing**



- **Static and dynamic code analysis**
  - **Data masking and encryption validation**
  - **Access control checks**
  - **Audit trail and logging verification**
- 

### **3. Automated Compliance Checks**

Some consultancies implement **automated test scripts** to continually validate compliance during development, especially in DevSecOps environments.

Examples:

- Automated scans for insecure data exposure
  - Tools like OWASP ZAP, Nessus, or Burp Suite for regular testing
  - CI/CD hooks to block deployments if non-compliant code is detected
- 

### **4. Gap Analysis & Risk Assessment**

They perform a **current state analysis** of your system and compare it to compliance requirements.

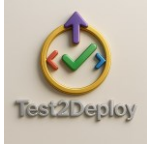
**Deliverables might include:**

- Risk heatmaps
  - Compliance matrices
  - Recommendations for remediation
  - Prioritized action plans
- 

### **5. Policy Review and Documentation Support**

Consultancies often assist in:

- Reviewing internal policies for compliance (e.g., consent handling, data retention)
- Documenting test results for audits
- Creating compliance reports for regulators or clients



---

## 6. Training & Awareness

We can also run workshops or awareness programs for your teams:

- **Secure coding practices**
  - **Privacy by design**
  - **Incident response protocols**
- 

### **Example Use Case:**

**A health-tech startup wants to launch in Europe.**

A software testing consultancy might:

- Test the app for GDPR compliance (data minimization, consent handling, right to be forgotten)
- Validate encryption of health records
- Perform a Data Protection Impact Assessment (DPIA)
- Ensure logs are immutable and meet audit requirements