# Vendor Assessment Questionnaire for GDPR Compliance Auditing

A **vendor assessment questionnaire** is essential for GDPR compliance auditing, helping organizations evaluate third-party data protection practices. It ensures that vendors adhere to GDPR requirements, mitigating risks associated with data processing and security. This structured approach promotes accountability and transparency in vendor relationships.

## Vendor Information

- Company Name:
- Contact Person:
- Email:
- Phone:
- Address:

## GDPR Compliance Assessment

1. **Data Processing Activities**
    - Describe the types of personal data processed on behalf of our organization.
    - Specify the purposes for data processing.
    - Is any special category data processed?
2. **Legal Basis and Documentation**
    - Do you have documented data processing agreements (DPAs) in place with your subprocessors?
    - Can you provide evidence of compliance with GDPR Article 28 obligations?
3. **Data Security**
    - Describe the technical and organizational measures implemented to protect personal data.
    - Is data encrypted at rest and in transit?
    - How is access to personal data controlled and monitored?
4. **Subprocessors**
    - Are subcontractors or subprocessors used in data processing?
    - List the subprocessors and locations where data is processed.
    - How do you ensure your subprocessors are GDPR compliant?
5. **International Data Transfers**
    - Is personal data transferred outside the European Economic Area (EEA)?
    - If yes, what mechanisms are in place (e.g., SCCs, adequacy decisions) to ensure compliance?
6. **Data Subject Rights**
    - What processes exist to support data subject access, rectification, erasure, and portability requests?
    - Do you support implementing the "right to be forgotten"?
7. **Data Breach Notification**
    - What is your protocol for detecting, reporting, and managing data breaches?
    - How soon can you notify our organization after a detected breach involving our data?
8. **Training and Awareness**
    - Do your employees receive regular GDPR and data protection training?
    - How is GDPR awareness maintained in your organization?
9. **Data Retention and Deletion**
    - What are your data retention and deletion policies?
    - Do you provide evidence or certification upon deletion of data?

## Declarations

☐ I confirm that the information provided is accurate, complete, and reflects the vendor's current GDPR compliance posture.

Vendor Representative: _____
Date: _____