

The Ultimate Assessment Checklist

1. Scope & Purpose

- ☐ Define objective of the assessment (e.g., compliance, risk mitigation, accountability).
- ☐ Identify the legal basis (GDPR, national laws, industry regulations).
- ☐ Specify the data processing activities under review.

2. Data Mapping & Inventory

- ☐ Identify the personal data involved (categories, sensitivity).
- ☐ Map data flows (collection, processing, storage, sharing, transfers).
- ☐ Define roles: Controller, Joint Controller, Processor.

3. Legal Basis & Compliance

- ☐ Verify if the processing has a lawful basis (Art.6 GDPR).
- ☐ If applicable, check for special category data (Art. 9) and appropriate safeguards.
- ☐ Assess compliance with transparency obligations (Art. 13 & 14 GDPR).
- ☐ If relying on legitimate interest, conduct a Legitimate Interest Assessment (LIA).

4. Risk Identification & Mitigation

- ☐ Identify risks to data subjects' rights and freedoms.
- ☐ Assess potential impacts (e.g., financial loss, discrimination, reputation).
- ☐ Consider threats (internal, external, technical, organizational).
- ☐ Implement risk mitigation measures (technical & organizational).

5. Data Protection Principles Review

- ☐ Data minimization: Are you collecting only necessary data?
- ☐ Purpose limitation: Is data being used only for specified purposes?
- ☐ Storage limitation: Are retention periods defined and enforced?
- ☐ Integrity & confidentiality: Are security measures in place?
- ☐ Accountability: Can you demonstrate compliance?

6. Vendor & Third-Party Considerations

- ☐ Identify data processors and sub-processors.
- ☐ Ensure Data Processing Agreements (DPAs) are in place (Art. 28 GDPR).
- ☐ Evaluate vendor security measures and compliance.
- ☐ Conduct a Transfer Impact Assessment (TIA) if data is transferred outside the EEA.

7. International Data Transfers

- ☐ Identify if data is transferred outside the EEA.
- ☐ Verify the transfer mechanism (e.g., SCCs, BCRs, adequacy decision).
- ☐ Conduct a Transfer Impact Assessment (TIA).
- ☐ Implement supplementary measures if needed (e.g., encryption, local processing).

8. Data Subject Rights & Accountability

- ☐ Ensure mechanisms for individuals to exercise their rights (access, erasure, portability, etc.).
- ☐ Have processes for responding to DSARs (Data Subject Access Requests).
- ☐ Ensure records of processing activities (ROPA) are up to date.
- ☐ Train employees on privacy compliance.

9. Security & Breach Readiness

- ☐ Assess security measures (encryption, access controls, pseudonymization).
- ☐ Verify incident response and breach notification procedures.
- ☐ Ensure breach logs and reporting mechanisms are in place.

10. Documentation & Continuous Monitoring

- ☐ Maintain detailed records of assessments and decisions.
- ☐ Document risk mitigation actions and follow-ups.
- ☐ Establish a review cycle for reassessments (e.g., annually or when processing changes).



Looking to expand your privacy knowledge?

Check out our English privacy resource library with free webinars, eBooks, and guides tailored for privacy professionals like you. Dive into topics from best practices to new privacy regulations and more!

[Explore the resource library](#)