10-STEP GDPR COMPLIANCE CHECKLIST FOR US COMPANIES

- [ ] **Build data privacy compliance into processes to reduce the risk of violations.** A privacy by design approach helps you remain compliant with the GDPR.

- [ ] **Document lawful bases for processing personal data.** Make sure every processing activity is clearly recorded and justifiable.

- [ ] **Set up clear procedures for data subject access requests (DSARs).** Ensure individuals can easily access, correct, delete, or transfer their personal data within GDPR timeframes.

- [ ] **Maintain a record of processing activities (RoPA).** Track what data you collect, where you store it, who accesses it, and how long it's retained.

- [ ] **Anonymize, pseudonymize, and encrypt all files.** This will help you protect personal data and uphold GDPR data subject rights.

- [ ] **Create an internal data security policy for employees and partners.** Ensure it covers all roles and responsibilities that involve handling data, and update it continuously.

- [ ] **Establish a process to implement data protection impact assessments.** This is required where data processing activities can result in a high risk to the rights and freedoms of individuals.

- [ ] **Regularly audit vendors and processors.** Confirm that third-party service providers meet GDPR standards and sign Data Processing Agreements (DPAs).

- [ ] **Establish a process to notify authorities of data breaches.** This must happen within 72 hours of a breach, per GDPR guidelines.

- [ ] **Appoint a Data Protection Officer (DPO) if required.** If your core activities involve large-scale monitoring or sensitive data, a DPO is mandatory.