GDPR Checklist for American Companies

The following questions represent the core components necessary for GDPR compliance. Please check off as applicable to self-evaluate your organization.

Governance

- ☐ Document your Privacy Governance Model
- ☐ Decide if statutory DPO is required
- ☐ Appoint local representative if no EU presence
- ☐ Personnel Training
- ☐ Review insurance coverage and adjust for higher fines/penalties under GDPR

Accountability

- ☐ Implement global overarching data protection policy
- ☐ Integrate privacy compliance into the audit framework

Fair Processing and Consent

- ☐ Ensure grounds for lawful processing are sufficient
- ☐ Ensure processing of sensitive personal data requirements are satisfied
- ☐ Ensure existing consents for processing personal data meet GDPR requirements
- ☐ Ensure systems allow withdrawal of consent

Notices/Vetting - HR

- ☐ Review and update employee notices to be GDPR compliant
- ☐ Conduct criminal record checks

Notices - Customers

- ☐ Review and update customer notices to be GDPR compliant
- ☐ Incorporate "child-friendly requirements" into notices

Children

- ☐ Ensure data processing notices directed toward children are "child friendly"
- ☐ Implement mechanism to seek parental consent

Data Subject Rights and Procedures

- ☐ Update privacy policy for dealing with requests
- ☐ Update internal processes for dealing with requests
- ☐ Ensure data subjects rights can be met with technical and operational processes

Record of Processing

- ☐ Identify all data processed in a detailed Record of Processing

- ☐ Implement and maintain processes for updating and maintaining Record of Processing

Privacy by Design and Default

- ☐ Embed privacy by design into apps and projects
- ☐ Create privacy impact assessment protocol

Complaint Contracting and Procurement

- ☐ Develop contract wording for customer agreements and third-party vendor agreements
- ☐ Identify all current contracts that require amendment under GDPR and develop process for amendment
- ☐ Ensure procurement process has controls to ensure privacy by design

Data Breach Procedures

- ☐ Review, update, or develop Data Breach Response Plan
- ☐ Review and update insurance coverage for data breaches due to higher GDPR fines
- ☐ Review liability provisions in agreements for breaches caused by service providers and other partners

Data Export

- ☐ Identify and updated all cross-border data flows and review data export mechanisms

*This checklist is composed of general questions about the measures your organization should have in place to state that you are in compliance with GDPR, and does not qualify as legal advice. Successfully completing this checklist **DOES NOT** certify that you or your organization is GDPR compliant.*