GDPR Compliance Checklist for US Businesses

GDPR compliance steps depend on whether the GDPR applies to your organization and how personal data is processed.

This checklist outlines the key GDPR requirements for US businesses.

- ☐ **Determine applicability:** Confirm whether your organization offers goods or services to individuals in the EU or monitors their behavior.
- ☐ **Identify your role(s):** Determine whether your organization acts as a controller, processor, or both.
- ☐ **Conduct a data mapping audit:** Document what EU personal data you process, where it is stored, who has access, how it is used, and how long it is retained.
- ☐ **Document a lawful basis for each processing activity:** Record the GDPR lawful basis that applies to each processing activity, such as consent, contract, legal obligation, legitimate interests, vital interests, or a task carried out in the public interest.
- ☐ **Update your Privacy Policy:** Include all information required by the GDPR, including lawful bases for processing, data subject rights, data sharing practices, international data transfers, and data retention practices, to meet GDPR transparency requirements.
- ☐ **Implement consent mechanisms:** Use consent forms, cookie banners, and similar tools that request consent before processing personal data where required. Ensure consent is freely given, granular, recorded, and as easy to withdraw as it is to give.
- ☐ **Establish DSAR procedures:** Set up a process for receiving, tracking, and responding to DSARs within the required timeframe.
- ☐ **Sign DPAs:** Enter into written agreements with vendors that process personal data on your behalf.
- ☐ **Appoint an EU representative and a DPO:** Appoint an EU representative if your organization is outside the EU but offers goods or services to individuals in the EU or monitors their behavior and no exceptions apply. Appoint a DPO if the organization is a public authority or body or its core activities involve large-scale monitoring of individuals or large-scale processing of special categories of personal data.
- ☐ **Implement security measures:** Protect personal data by implementing appropriate technical and organizational security measures, such as encryption, access controls, MFA, and security monitoring.
- ☐ **Establish data breach response protocols:** Develop a plan for responding to personal data breaches, documenting incidents, determining whether notification is required, and reporting breaches within **72** hours when required.
- ☐ **Implement safeguards for international data transfers:** Identify transfers of personal data outside the EEA and implement an appropriate transfer mechanism, such as certification under the EU-US DPF or the use of SCCs.
- ☐ **Conduct DPIAs:** Complete a DPIA before carrying out processing activities that are likely to result in a high risk to the rights and freedoms of individuals.

- ☐ **Provide GDPR training:** Train employees on GDPR responsibilities, data protection practices, and security procedures, and conduct regular compliance audits.
- ☐ **Maintain ROPA:** Keep records describing processing activities, including processing purposes, categories of personal data, recipients, international data transfers, retention periods, and security measures.