usercentrics

GDPR Checklist for US Companies

September 2021

DISCLAIMER

These statements do not constitute legal advice. They merely serve to support and inform you about the current legal situation. Please consult a qualified lawyer should you have any legal questions.

GDPR Checklist for US Companies

Make data privacy and protection a key consideration in all aspects of development and operations. Building in compliance is more efficient, cheaper, and less resource-intensive than retrofitting it. Especially if a company ends up with fines for violations.

Create an internal security policy for employees, partners, and contractors and keep it updated. Ensure that it is clear and comprehensive to the company's operations and specific roles within the organization where accessing personal data is necessary.

Know what a data protection impact assessment is and have a process to carry it out.

Wherever possible when personal data is collected, anonymize, pseudonymize and encrypt it.

Have a process in place to notify data subjects and the correct authorities within the required time frame in the event of a data breach.

Requirement	Key Actions	Details
	Operations	

Know what data you collect, store, and use	• Conduct an information audit to learn and document:
	  ○ what data you collect
	  ○ why it is collected
	  ○ who has access to it (including third parties)
	  ○ how and where it is stored/protected
	  ○ how long it is kept
	  ○ how it is expunged
		• Organizations with 250+ employees, or that conduct higher-risk data processing must keep an up-to-date and detailed list of their processing activities, which can be shown to regulators on request. (Companies with fewer than 250 employees should still do these audits and maintain this information.)

Have a legal basis for data processing activities	• Determine under which legal basis you process data. • Determine what additional conditions may apply. • Document the rationale for your organization's chosen legal basis and be prepared to present it to regulators.	• Legal basis is determined based on the six conditions under Art. 6. • There are additional provisions relating to children and special categories of personal data in Arts. 7-11. • Be aware of the extra obligations if consent is your chosen legal basis.

Requirement	Key Actions	Details

Appoint appropriate officers and representatives to manage data privacy and protection initiatives.	• Designate a privacy/compliance officer in your organization.
	• Appoint a representative within the EU if your organization is outside (e.g. US).
	• Determine if your organization needs a Data Protection Officer, and appoint one if required.
		• The internal officer needs to be able to understand the needs of ongoing compliance, work on drafting, reviewing, implementing and enforcing the policies.
		• Processing data of people in particular EU member states requires a representative in each country who can communicate on your behalf with data protection authorities.
		• A Data Protection Officer is needed if the organization:
		  ○ is a public authority
		  ○ large scale data processing is a core activity
		  ○ large scale data processing of special categories' data is a core activity.

Create and use a data processing agreement with third parties.	• Any third parties that process data on your behalf need to sign a data processing agreement that clearly outlines how data is to be transferred, stored, protected, used, and erased.	• This can include email hosting, cloud services, analytics software, etc. • Ensure rights and obligations of both parties are clear. • Reputable services should have a data processing agreement for review on their websites.
Users and Customers		
Duty to provide information	• Let users know clearly that you are using cookies or other tracking technologies on your website.	• Include the following information in the Privacy Policy: ○ Name and contact of data controller

Requirement	Key Actions	Details
	• Explain what the tracking technologies are doing and why (purpose). • Include this information in a Privacy Policy that is easy to find, read, and understand. • Review and update the Privacy Policy at least every 12 months.	○ Purpose of data processing/tracking technologies ○ Categories of users and personal data; ○ Transfers of personal data to third countries; ○ Time limit of deletion of personal data; ○ General description of security measures (to be prepared for e. g. against cyberattacks)
Obtain explicit consent	• Obtain users' explicit consent to use tracking technologies and to store cookies on their device(s).	Consent must be: • **Explicit**: active acceptance, e.g. ticking a box or clicking a link • **Informed**: who, what, why, for how long? • **Documented**: you have the burden of proof in the case of an audit • **In advance**: no data is to be collected before opt-in, e.g. cookies cannot be set on your website before the user has consented to them • **Granular**: individual consent for individual purpose, i.e. consent cannot be bundled with other purposes or activities • **Freely given**: e.g. "Accept" and "Reject" button or equal size and prominence • **Easy to withdraw**: opt out on the page, and easily accessible later if user changes their mind **Exception:** strictly necessary cookies (aka essential cookies)

GDPR Checklist for US Companies

Requirement	Key Actions	Details
Setting cookies	• Collect and process data with cookies only with valid consent.	• **Loading**: ensure cookies are not loaded until the user has given consent • **User Refusal**: if a user rejects cookies, no cookies can be set, however, users should still be allowed to use your website/access your service even if they refuse to allow the use of certain cookies.
Legally compliant documentation	• Document and store consent received from users.	• **Data Protection Authority (DPA) Audit**: comply with documentation obligations and be able to demonstrate users' consent in case of an audit by data protection authorities.
Opt out	• Rejecting the use of cookies or other tracking technologies must be as easy to access and use as consenting.	• **Easy in, easy out:** it must be as easy for users to withdraw their consent at any time as it is for them to give it. • **External links**: linking to a separate page for opt out is not sufficient. • **After Opt-out**: ensure that no further data is collected or forwarded from the moment the consent request is rejected or rescinded, i.e. the opt-out must also be technically linked to the cookie and, ideally, documented.