



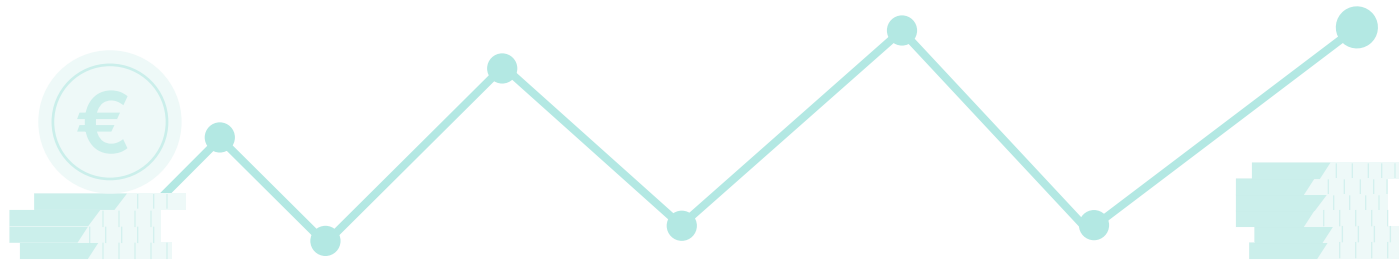
# 7-Step GDPR Compliance Checklist

A Roadmap for EU, US & Other Global Marketers

# 7 Key Steps to Compliance

Strict GDPR regulations affect all companies, regardless of whether they are based in the EU or US.

Compliance can be difficult because of the complexity of information available.



This 7-step checklist acts as a roadmap to meeting your requirements, and is equally applicable to other privacy laws such as CCPA, PIPEDA etc.



Any business with personal data on even one EU citizen or a website accessible in the EU is liable for GDPR non-compliance fines.

## 78%

US Companies Working to Comply With GDPR (OVUM)

## €1,5Bn

Total GDPR Fines (Privacy Affairs)

## \$385Bn

Value of GDPR Compliance Market

Source: [INSIGHT.com](https://www.insight.com)

# 1. Raise Awareness About GDPR

I started European Alternatives to show that there are good alternatives to the big US tech companies and because it bothered me that they are so hard to find.

Especially in times of GDPR and problems with data transfer between USA and EU, many people are rightly looking for European alternatives and I wanted to help them.



**Constantin Graf**  
Founder, [european-alternatives.eu](https://european-alternatives.eu)

Ensure that all key people at your company understand the impact of GDPR.

Identify areas where GDPR compliance problems are likely.

Assess the implications of compliance measures on company resources.

Get board-level support.



## 2. Designate In-House Responsibility



Consider whether you need a formally designated DPO or an external advisor.

Assess where this role will sit within your company structure.

Appoint someone to take charge of data protection compliance.

### When do you need to hire a DPO?

According to GDPR, a company must appoint a DPO if they meet any of the following conditions:



Data is processed by a public authority.




Data undergoes systematic monitoring.



Data is processed at a large scale.



Data processing operations are centralized.

 If your company does not have an office in the EU, you must appoint an official representative in the Union.

# 3. Plan Your GDPR Compliance Project

Identify your EU data protection authority — or for multinationals, the lead DPA.

Assess whether data protection by design is incorporated into processes.

Evaluate data requirements and ensure nothing else is collected.

Establish the legal basis for data processing activity.

Create a GDPR Diary (or Data Register), recording how you comply with GDPR.

Review company insurance policies against the higher GDPR fines and penalties



# 4. Review Personal Information on Hold

Document the personal data on file, where it's from and who it's shared with.

Begin building and maintaining accurate records of all personal data:


Create a record of personal data processing activities.

Identify all cross-border data transfers and review processes.

Establish whether age verification of data subjects is required.

## Category of Information to Collect:

- Source of personal data.
- Reason for collecting data.
- Proof of user consent.
- Type of personal data.
- How data is processed.
- When data is discarded.

 GDPR Regulations only allow companies to process the data of people aged 16 and older. For anyone younger, the parent or guardian must provide companies with the consent they now need by law.

# 5. Assess Risk in Operations & Processes

Risk assessments are crucial to GDPR compliance planning, enabling companies to develop effective processes, establish contingency plans and manage the risk.

Create a map showing how data flows to, through, and from your organization.

Identify risks from the map - particularly from third-party involvement.

Do a Privacy Impact Assessment (IPIA) if required.

Do a Data Protection Impact Assessment (DPIA) if required.

Ensure procedures in place to detect, report and investigate a data breach.



Technology companies have embraced the new realities around personal data collection, storage, and processing. It took some adjusting in terms of AI profiling, lead-generation strategy, as well as tools and systems to guarantee compliance, but I think we're past the panic moment of May 2018.

**Andreea Munteanu**

Head of Marketing & Communications  
Promus Ventures





## 5. Review Personal Information on Hold



Identify when you'd need to notify the SA or affected individuals.

Document data protection measures.

**Impact assessments are compulsory when the data is highly sensitive, like:**

- User location tracking.
- User behavior tracking.
- Associated with children.
- Used for automated decisions with legal consequences.
- Monitoring publicly accessible areas.
- Processing of personal information



# 6. Develop Policies, Procedures & Processes

Create a thorough, clear and easily accessible privacy notice.

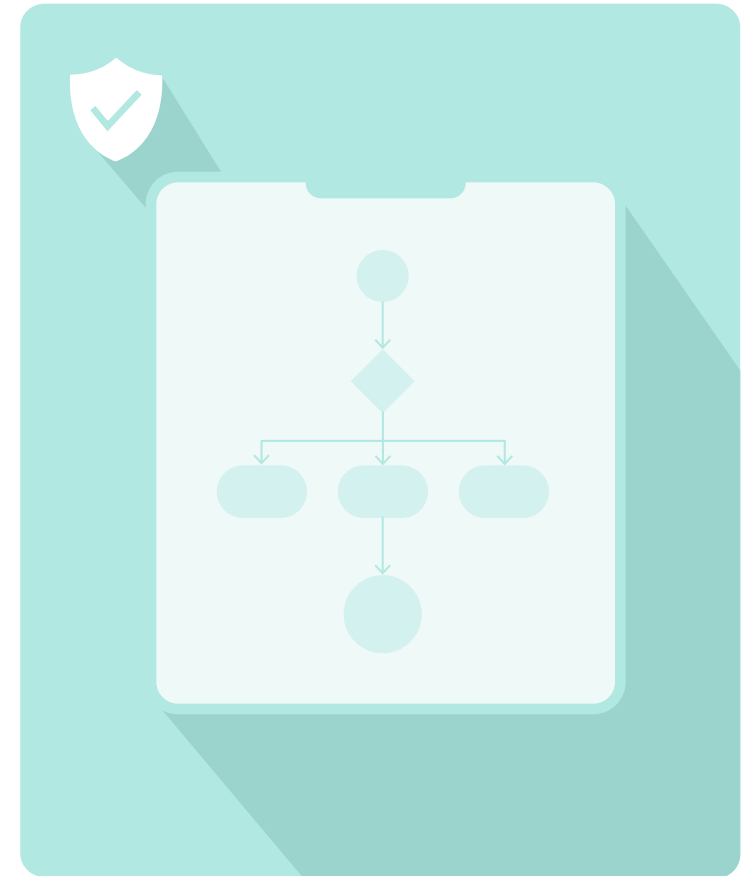
Ensure data protection policies meet GDPR requirements.

Adjust privacy controls to meet rules regarding privacy by design.

Ensure you have explicit consent for data collection, retention & erasure.

Review employee, customer and supplier contracts and update them if necessary to cover personal data processing.

Have an information security policy in place.





## 6. Develop Policies, Procedures & Processes



### **Review the privacy rights of your customers. It must be easy for them to:**

Request and receive all information you have about them.

Correct or update incomplete or inaccurate information.

Request to have their personal data deleted.

Ask you to stop processing their data.

Receive a copy of their personal data in a format that can easily be transferred to another company.

Object to the processing of their data.

# 7. Keep Auditing & Monitoring Compliance

**GDPR compliance will prove to be an ongoing project for companies, and you should carry out regular audits and training to meet privacy regulations.**



Schedule regular audits of data processing activities and security controls.

Continue training staff on secure, GDPR-compliant data processing.

Keep records of personal data processing up to date.

Document your ongoing compliance, auditing and record keeping.

Undertake DPIAs where required.

Assess data protection practices and manage some of the more demanding elements of GDPR compliance.

visitor**analytics**

# Privacy First Website Analytics

✔ With more than 2 million active users from 190 countries and offering an all-on-one website statistics toolkit for any business, **Visitor Analytics** is one of the leading online analytical solutions worldwide.

✔ All features are **100% GDPR/CCPA compliant** and data is collected in real time.

[Register today for a free trial →](#)



Disclaimer: The vendors of Visitor Analytics SRL give notice that this document is produced for the general promotion of the software only and for no other purpose. Receipt of these particulars do not form part of any contract and are for guidance only and have been prepared in good faith to give a fair overall view of the software and martech landscape and are believed to be correct as at the date of publication. The content relating to the past and/or current performance of the software is not necessarily a guide to its performance in the future. Prices quoted may be based on a conversion rate when the document was created and may vary.

Copyright © All content in this document, including without limitation, logos, text, images, graphics etc are protected by copyright and/or design right owned by Visitor Analytics SRL. No license is granted to copy, reproduce, use or otherwise deal in Visitor Analytics content, including any copyright or design right work of Visitor Analytics.