How to comply with GDPR in the U.S.

A guide for U.S. businesses with global aspirations and reach

WIPFLI

GDPR has global reach

Are U.S. companies beholden to European Union (EU) laws? In the case of GDPR, yes.

The General Data Protection Regulation (GDPR) is a law meant to protect the data and privacy of individuals in the EU. Any organization that processes personal data of EU citizens or residents must comply with the regulation, regardless of where it operates. Companies that fail to follow GDPR principles are subject to sanctions and fines — up to 20 million euros or 2-4% of global revenue.

"Processing" and "personal data" are broad terms. So, how do U.S. companies know whether GDPR applies to them?

Use this guide to start your analysis. It covers:

- GDPR definitions and scope.
- How to determine if GDPR applies to your company.
- What to do if you're subject to GDPR.
- A GDPR compliance checklist for U.S. companies.

As of December 2022, GDPR has levied

1,216 fines.

Together, they exceed

$2.5 billion

in penalties, according to Enforcement Tracker.

The three biggest fines GDPR has issued have gone to U.S. companies.

AMAZON
was fined
$781 MILLION
in 2021 for not obtaining consent from users before storing advertising cookies.

INSTAGRAM
was fined
$427 MILLION
in 2022 for publishing kids' phone numbers and emails.

FACEBOOK/META
was fined
$275 MILLION
in 2022 after personal data was found in an online hacking forum.

GDPR definitions and scope

GDPR is unusual because it has a wide geographical scope. The law is intended to keep EU citizens and their data safe, regardless of where they shop or do business. That's called the "extraterritorial effect."

Any organization that processes personal data of EU citizens or residents must comply with the regulation. Within the scope of GDRP are:

- **Processing:** This includes data collection, storage, transition and analysis. GDPR applies to companies that use the data (i.e., data controllers) and those that handle it (i.e., data processors).
- **Personal data:** This is any information that could be used to identify an individual, either directly or indirectly.

U.S. companies are subject to GDPR if either of these two conditions are met:

1. They offer goods and services to people in the EU.
2. They monitor online behavior of people in the EU.

Offering goods or services

Any business that offers products or services to people in the EU should be GDPR compliant. Regulators look for signs that you cater to EU citizens, such as advertising in German or including pricing in euros.

Regulators aren't interested in occasional exchanges. But pay attention. If transactions with the EU increase or EU citizens become a target market, then you must comply with GDPR.

Monitoring behavior

Does your company monitor web traffic? Or collect email addresses? That's personal data.

U.S. companies are subject to GDPR if they collect or manage any data about EU citizens/residents for any professional or commercial reason, even if the company doesn't have an explicit EU connection (e.g., an office, staff or bank accounts).

Other considerations

Small- and medium-sized businesses may think they're exempt from GDPR — but that's not true. Thresholds are different, and some requirements, such as record-keeping, are less strict if you have fewer than 250 employees — but the law still applies.

GDPR applies to:

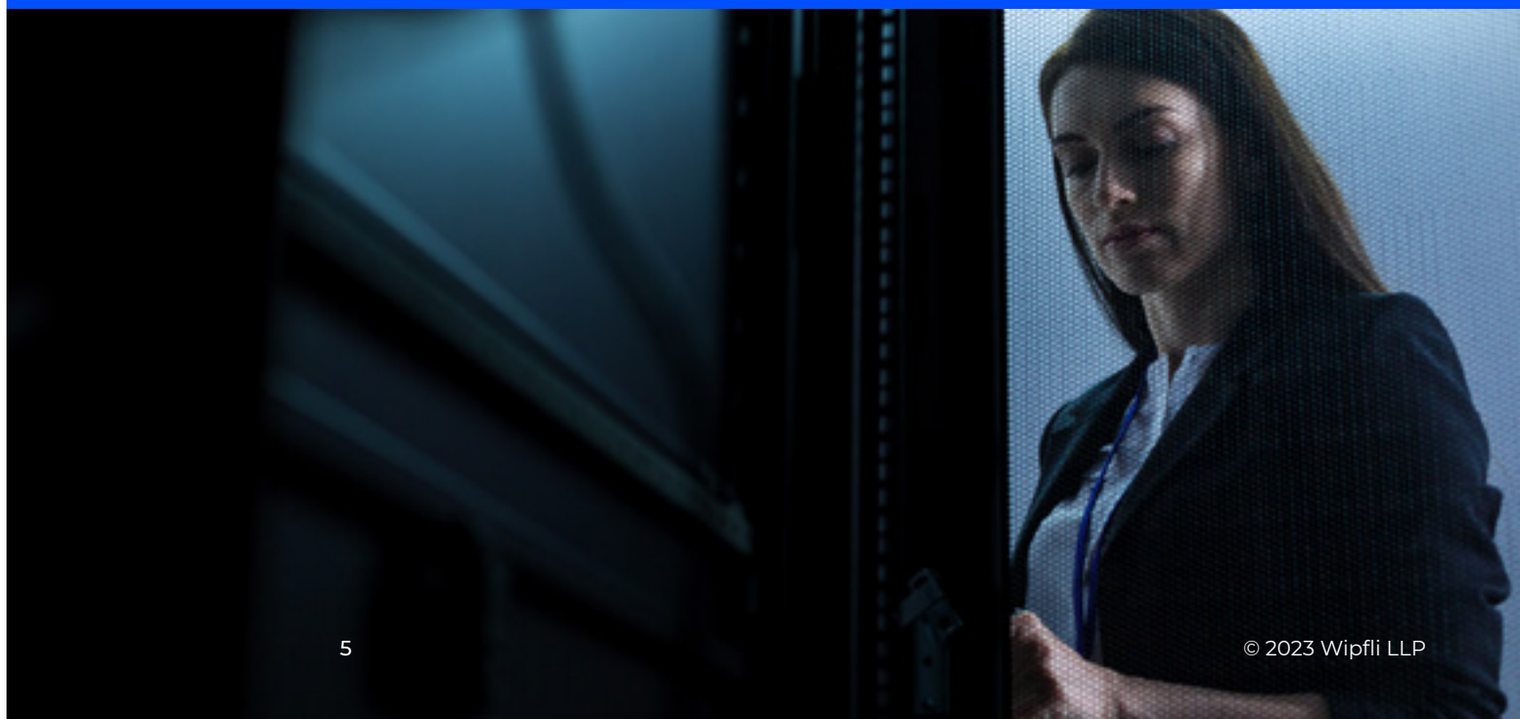
- Nonprofit and for-profit organizations.
- Companies of nearly every size.
- Companies that employ EU citizens or residents.
- Companies that manage consumer data files in or from the EU.
- Companies that move consumer or employee data outside the EU, either directly or through a third party.

This guide is a starting point. Make sure you read and understand the regulation, including definitions, compliance components and privacy procedures. Assign a compliance leader or work with a GDPR expert for help.

What's "personal" in the GDPR?

GDPR covers information that's collected for marketing purposes, such as political opinions, demographic data or views on specific issues. Any personal data that can be combined with other data to identify an individual is also covered under GDPR, such as:

- Names
- Social networking posts and profiles
- Government identification numbers
- Online information (e.g., IP addresses and device IDs)
- Mailing addresses
- Telephone numbers
- Email addresses
- Credit scores
- Photos
- Medical information
- Bank account details



How to determine whether GDPR applies to your company

Once you understand the definitions and activities addressed by GDPR, examine your operations. A thorough internal assessment has three components: communication, review and documentation.

Communicate

Communicate with your management team. Make sure they understand how GDPR applies to your business. Then, identify individual teams or processes to analyze for potential exposure.

Consider third-party vendors and relationships at this stage. You may need to include them in your communications and analysis, too.

Review

Does your company:

- Have employees working in the EU?
- Offer services or goods to individuals in the EU?
- Monitor the activities or behaviors of covered individuals?

If you can answer yes to any of these questions, then GDPR applies to your U.S. business.

If you're not sure, take a detailed look at personal data you control, where it's located and how it's secured. If any of your data pertains to EU citizens/residents, then you must adhere to the privacy principles outlined in GDPR.

Document

Document your analysis process, the data you examined and the result. If you determine that your organization is not subject to GDPR, continue to monitor compliance as new products, services and markets develop.

What to do if your company is subject to GDPR

If GDPR applies to your business, take these steps:

1. Establish a governance process

Start by assembling an internal team and a data protection officer (DPO). The DPO will become the company's GDPR expert. They are also the main point of contact for the data protection authority. Regulators recommend appointing someone who's knowledgeable about IT and law.

Write the first draft of your GDPR policies and procedures, and discuss how GDPR will affect business processes. Then, set a timeline for GDPR compliance. You'll also need a detailed action plan, a timeline and a budget.

2. Conduct a comprehensive risk assessment

Audit all the consumer data you have, use, acquire and store. Then, categorize it. For example, you could create data categories for personally identifiable information and for sensitive versus nonsensitive data. Note the locations where data is controlled and processed and whether it's internal or by third-party vendors.

3. Design controls

When you have a handle on the data and its location, start to design controls.

Remember, GDPR gives people more control over how their data is collected, used and protected. That means you need to address consent, individual data rights and security.

- **Consent:** Get informed/affirmed consent to process data, including explicit parental consent for minors' personal data. Keep in mind: The definition of "minor" varies among EU countries. You may need explicit consent to process special categories of data, too (e.g., biometric data).

- **Data rights:** EU individuals have a right to access their data, have it corrected and even have it erased. They also have control over how their data can be used and whether it's "portable." Establish procedures and business tools to enable secure access.

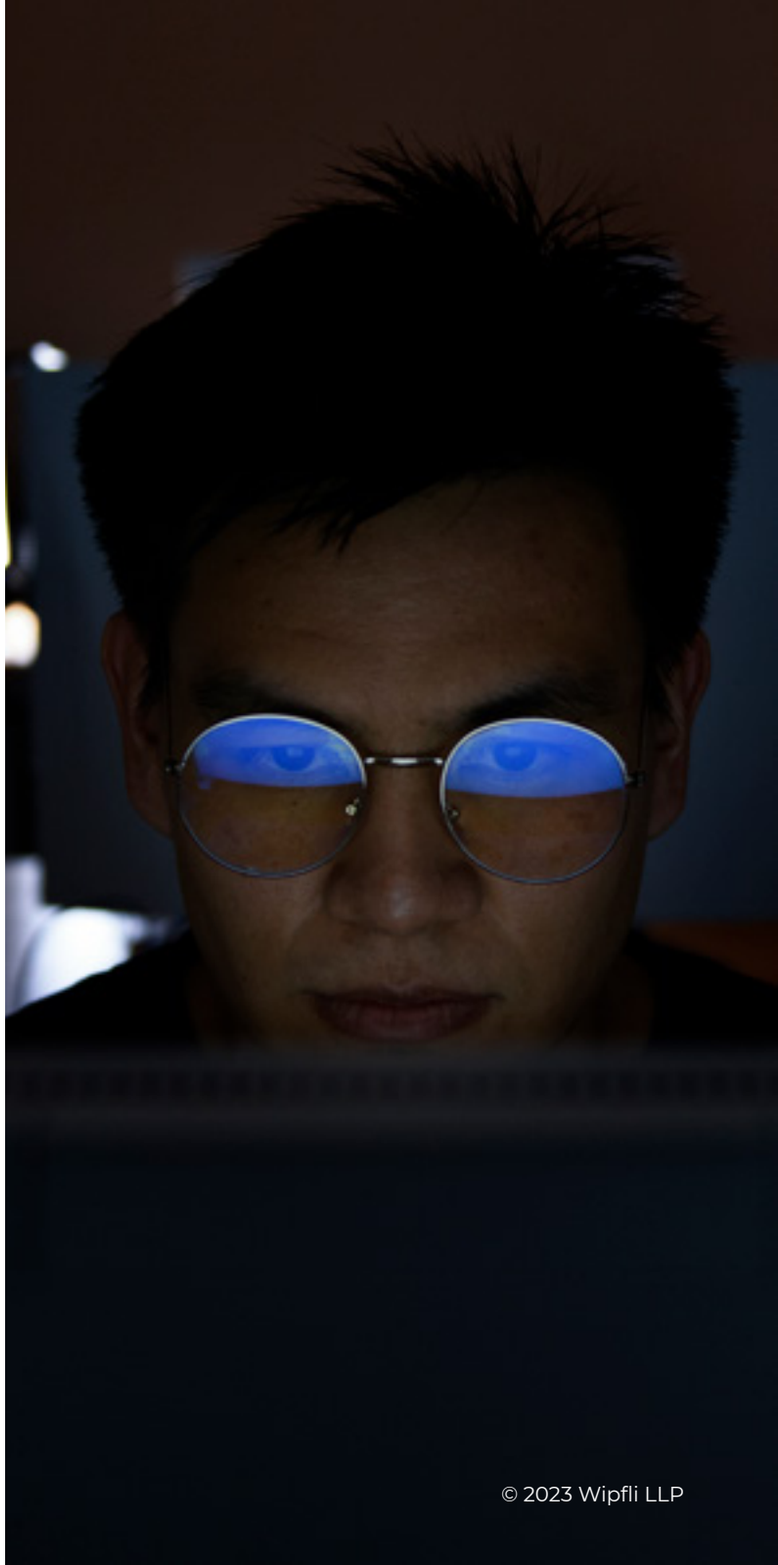
- **Security:** If your company moves data between EU and non-EU countries, you'll need mechanisms to secure the transfer. Technical and physical controls should protect the data throughout capture, storage and disposal. Practices to ensure data quality and integrity also support compliance.

4. Formalize GDPR policies, procedures and processes

After the assessment, update your policies and procedures. Cascade the requirements and changes across the organization. It's important that staff understand how to handle EU citizens' and residents' data.

5. Test your controls

Develop a process and schedule to test compliance. The internal team should monitor consumer data practices, as well as new vendor or partner relationships. An independent auditor can test your GDPR program to identify knowledge gaps and weaknesses.



A GDPR compliance checklist for U.S. companies

☐ Audit for EU personal data

If you process personal data, determine whether it belongs to people in the EU. If it does, decide whether the processing activities are related to offering goods or services. (See Recital 23.)

If you process personal data of EU citizens or residents:

☐ Tell consumers why you're processing their data

You're required to provide clear and transparent information about your activities. In most cases, this means you need to update your privacy policy. However, consent is only one of the legal bases that can justify the use of personal data, and extra duties may be required. (See GDPR Article 6, GDPR Article 12, consent requirements and privacy notice.)

☐ Assess your data processing activities to improve protection

Assess the security and privacy risks associated with the data you process, and create ways to mitigate those risks. Implement data security practices, such as end-to-end encryption, to limit your exposure. Start all new projects under the principle of "data protection by design and default." (See GDPR Article 25.)

☐ Establish data processing agreements with vendors

Document the rights and responsibilities of every vendor that handles personal data for you. That includes email vendors, cloud storage providers and subcontractors. (See the Data Processing Agreement Template.)

☐ Appoint a data protection officer and representative

Many organizations are required to designate a DPO. The GDPR specifies some of the qualifications, duties and characteristics of this management-level position. (See Everything you need to know about the DPO.)

Some non-EU organizations are also required to appoint a representative who is based in an EU member state. (See Article 27 for requirements and Recital 80 for details about the representative role.)

☐ Know what to do if there's a data breach

If personal data is exposed, you are obligated to notify customers. Articles 33 and 34 outline your responsibilities for notification and communication following a data breach.

Source: gdpr.eu

Need a guide?

If you're not sure how GDPR affects your business — or plans for growth — we can help. Wipfli can assess how the regulation affects your company, help put a DPO in place and design a GDPR-compliant privacy program. We can also train employees on GDPR requirements, including incident and data breach response.

Think you've got it under control?

Good. Wipfli can perform readiness testing or an independent audit to ensure your GDPR practices are performing as planned. Our knowledge and experience can protect your business — and customer data — and help you avoid serious penalties.

Learn more ▸

wipfli.com/GDPR

Perspective changes everything.

WIPFLI