How GDPR Impacts Marketers: What You Need to Know

Shares 671

Are you confused by the European Union (EU) General Data Protection Regulation (GDPR)?

Wondering how GDPR affects your marketing?

In this article, you'll **find a plain-language overview of GDPR, how it could impact your data collection, and what you need to do to make sure you're compliant before May 25, 2018**.

How GDPR Impacts Marketers: What You Need to Know by Danielle Liss on Social Media Examiner.

What Is GDPR?

The General Data Protection Regulation (GDPR) is a European Union (EU) law taking effect on May 25, 2018. GDPR is designed to give greater protection to an individual's personal information and how it's collected, stored, and used. There are strict requirements placed on companies that possess the personal data of people located in the EU.

Potential Fines

After May 25, 2018, organizations that aren't in compliance with GDPR's requirements could face large fines (up to 4% of a company's annual global turnover or €20 million), which vary based on the severity of the infraction.

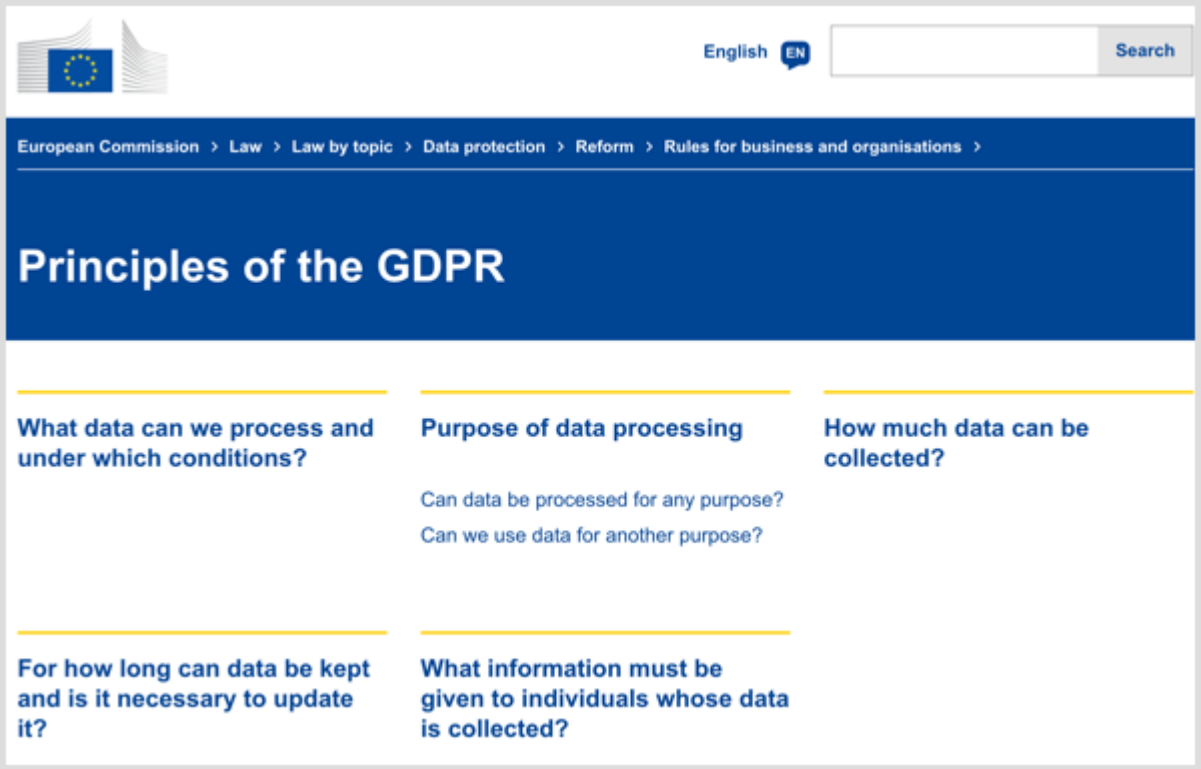
When Does GDPR Apply?

A financial transaction isn't necessary for the GDPR to apply. A non-EU-based business must comply with the GDPR if it

collects or processes personal data of any EU resident (EU citizenship is not required).

Personal Data

Under GDPR, personal data is defined as information that can be used to identify someone, directly or indirectly. This includes IP address, cookies, location data, name, and email address.



GDPR may require significant changes in how a company discloses and obtains consent to collect personal data.

#1: What Is Required Under GDPR?

Explicit Consent

If you're collecting personal data from an EU resident, you must obtain explicit consent, which generally means that consent should be:

- **Voluntary**. Have the user take affirmative action.
- **Specific and informed**. Make sure people are aware of

what you're collecting, how it's being used, and whom it may be shared with.
- **Unambiguous**. Don't disguise with redirects to terms of service overflowing with legal jargon.

More specifically, for consent to meet GDPR standards, it must:

- Contain a clear statement of consent, using plain language that's easy to understand (no legalese).
- Require a positive opt-in (i.e., no pre-ticked boxes, silence, or inaction).
- Be separate from any other terms and conditions.
- Explain why the entity wants the data and what it will do with the data.
- Name any third-party controllers that will rely on the consent.
- Explain how the data subject may withdraw consent.
- Avoid making consent a precondition of service.



When the processing of personal data has multiple purposes, individuals must be informed of each purpose and allowed to consent or decline each purpose separately. Additional requirements apply when obtaining consent from children. Entities must also keep records of consent obtained from data subjects.

Strict Privacy by Default

Strict privacy settings should be the default setting. A user shouldn’t have to go into their settings to make manual changes to opt into stricter settings.

Rights to Data

Under GDPR, individuals have greater control over how their personal information is collected, stored, and used. Individuals have a right to access their data, which means the right to know where, why, and how their data is processed. This includes the right to request a report to access their data. Additionally, individuals have a right to be forgotten, which means their data can be deleted.

Breach Notification

Organizations have a duty to report certain types of data breaches to the relevant supervisory authority within 72 hours, unless the breach is harmless and poses no risk to the individual. If a breach is concluded to be high risk, the company must also inform the individuals impacted.

Appointment of Data Protection Officer

In some cases, companies must appoint a data protection officer. This is required when: 1) an entity regularly monitors sensitive personal information (e.g., race, genetic data, etc.), 2) an entity regularly monitors personal data on a large scale, or 3) is a public authority.



Information of Children

Under GDPR, a company may not collect personal data of anyone

under 16 without parental consent. Implement a process to verify age and to obtain parental consent when necessary.

Takeaway: Under GDPR, companies must ensure that they have clear policies in place to maintain compliance.

#2: How Does GDPR Impact Non-EU Companies?

For many social media marketers, there are many questions about whether compliance is necessary for companies outside of the EU. However, non-EU companies must comply with GDPR if: 1) they collect or process personal data of any EU resident, or 2) the company's activities relate to offering goods or services to EU citizens, regardless of whether payment is required.

This compliance is mandated for any EU resident, regardless of EU citizenship. Even an American citizen who's only temporarily located in the EU is protected by GDPR.

Remember that a financial transaction isn't necessary for the GDPR to apply. Any non-EU-based business must comply with the GDPR if it collects or processes personal data.

Takeaway: All companies must obtain explicit consent from the data subject, including non-EU companies. Simply being located outside of the EU doesn't relieve a company of compliance.

#3: GDPR Compliance Action Plan for Social Media Marketers

Audit and Implement GDPR Compliance Strategy

First, conduct an audit of your website.



- Determine what data you hold, where it came from, and whom you share it with.
- Determine what information you have pertaining to existing EU residents.
- Review which third-party service providers you use and ensure they're GDPR-compliant.

After you've completed the initial audit, **review all information** to **determine what you need to do to comply with GDPR**. Next, **prepare an action plan to update your privacy policy and methods for obtaining consent**.

Update Your Privacy Policy

Ensure your privacy policy is updated to address GDPR. **Discuss what information you collect, how it's used, and any third-party service providers you share the information with**. Include the process to follow to invoke the right to access personal data or the right to be forgotten.

Remember, while your privacy policy will reference the requirements of GDPR, having it installed *doesn't* mitigate your need to obtain informed consent.

Obtain Explicit Consent

After you've determined what personal information you collect or process, obtain explicit consent, described above, for each reason you collect such data. For instance, if you use cookies for affiliate links and a Facebook pixel, you'll need explicit

consent for each use.

Takeaway: The goal of your GDPR strategy will first help you determine what personal information you collect and then put new procedures into place to ensure compliance.

#4: Potential Areas of Concern for Social Media Marketers

If you still aren't sure exactly what personal data you may be collecting, here are a few examples that are common for social media marketers, along with some tips on how to stay compliant for each.



Google Analytics

If you use Google Analytics, you may be collecting user ID/hashed personal data, IP addresses, cookies, or behavior profiling. To be GDPR-compliant while using Google Analytics, either 1) anonymize the data before storage and processing begin, or 2) add an overlay to the site that gives notice of the use of cookies and asks for the user's permission prior to entering the site.

Retargeting Ads and Tracking Pixels

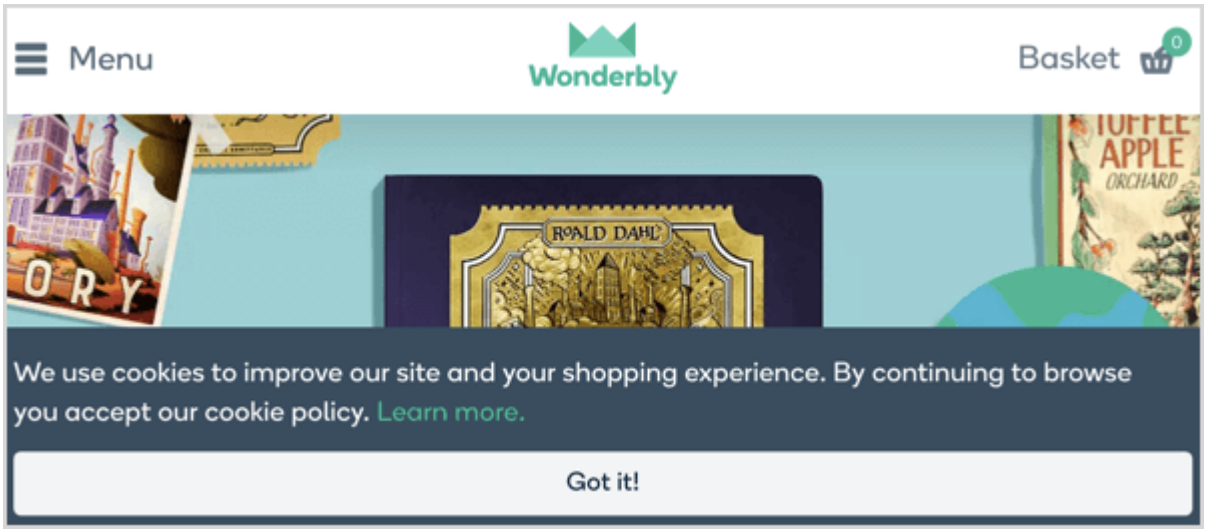
If your website uses remarketing ads, including the Facebook pixel, **inform website visitors of this immediately** when they enter your site and **obtain informed consent**.

If you publish sponsored content, **ask your client if they use tracking pixels or cookies and why**. If the company uses pixels or cookies to capture personal information or to remarket to

your audience, you must **get consent from visitors immediately** when they enter your site.

Email Opt-In

On the subscription form, **have a checkbox for the visitor to consent to everything they're about to subscribe to**. If your newsletter uses tracking pixels to see when they open it, put a visible disclaimer before they subscribe. Verify if your email service provider offers GDPR tools.



Affiliate Links

If you use affiliate links, you need to **get consent for cookie usage**. You can gain consent on an individual post or as an overlay. Consent must come before the visitor clicks the affiliate link because a cookie will be placed on their browser to track sales activity.

Display Ads

If you have ads on your website from a third-party ad server, upon entering your site, users should immediately consent to your use of a third-party server that collects user data for advertising and marketing purposes. If your ad server uses cookies to gather data on the visitor for targeting purposes, **inform visitors upon entering your site** and **get consent for using cookies for this purpose**.

Contact Forms

Before users submit their information in a contact form, **get their explicit consent with a checkbox**.

Comments

Before users can leave a comment, **get consent by using a checkbox** and **disclose that your site will store their comments and, as needed, information relating to the comment** such as the date and computer's IP address. Let them know how the information is used. Also, include a reminder that some information may be displayed publicly, such as name or URL, if they're submitted with the comment.

Product Sales

If you're selling services or products to EU residents, **only collect necessary information from your customers upon checkout** and obtain explicit consent prior to submitting the purchase to **let them know how you'll use that information**.



Takeaway: Ensure that you **obtain consent for each purpose of the data collection** (e.g., one checkbox may say that they authorize being added to your mailing list and another consent to having personal data stored for communication about purchases).

Remember, if you aren't sure about what type of data a plugin or marketing tool collects, investigate it with the developer to **ensure that you're not using non-compliant tools**.

#5: Plugins to Help You Manage GDPR

If you’re looking for tools to help you manage GDPR compliance, here are a few WordPress plugin options:

- GDPR: a nearly all-in-one solution with options for consent management, privacy policy configurations, fulfilling data export requests, and more.
- Shariff Wrapper: prevents the automatic transmission of data via sharing plugins.
- GDPR Personal Data Reports: generates a personal data report for users invoking their Right of Access.
- Wider Gravity Forms Stop Entries: allows Gravity Forms users to stop sensitive information from being stored on their servers.
- Delete Me: allows users to delete their own accounts and profiles.

Conclusion

Ready or not, GDPR is coming and you need to be compliant by May 25, 2018. Even if you’re a non-EU company, GDPR is likely going to impact your social media marketing business; however, by following a few simple steps, you can ensure your compliance.

What do you think? What steps have you taken to make your business GDPR-compliant? Please share your thoughts in the comments below.



How GDPR Impacts Marketers: What You Need to Know

www.SocialMediaExaminer.com

Shares 671

How GDPR Impacts Marketers: What You Need to Know