Ogilvy & Social.Lab

GDPR:
What social media marketers need to know

GDPR: What social media marketers need to know

The EU's General Data Protection Regulation (GDPR) has been constantly positioned as disruptive for personalised marketing and challenging for businesses to grapple with.

Now that the regulation has been officially implemented, the actual impact for advertisers and agencies becomes more tangible.

For social media marketers - who are at the centre of this – there are two major implications. First, since all major platforms have updated and built-in privacy policies, it is essential to understand who actually needs to be compliant. And secondly, educating users about their new rights, while ensuring a seamless experience will be of utmost importance.

We summarize some key takeaways regarding the GDPR specifically on social, debunk a few myths and give an overview of the most relevant changes per platform.

In a nutshell

- **In practice** the GDPR means that when collecting user data, advertisers will have to comply with stricter requirements regarding consent (whether it's explicit or unambiguous). In other words, the user will have more control by giving affirmative opt-ins.
- **The territorial scope** of the latest regulation applies everywhere for companies that process data from European citizens. But do keep in mind: even if the company is not European, as soon as it sells to EU citizens, it is also subject to GDPR.
- **The obligations** for all involved parties depends on what exactly they do with personal data. The regulation defines two distinctive roles: data controller and data processor. It all comes down to understanding your role and checking if you're playing according to the rules:

Data controller	Data processor
If your company / organization decides 'why' and 'how' the personal data should be processed it is the data controller.	The data processor processes personal data only on behalf of the controller. The data processor is usually a third party external to the company

- **In case of a data breach**, you have 72 hours to report this to the controller and the supervisory authority of the Member State. In case of highly sensitive data, the users should be alerted as well.
- **The implications** for being noncompliant vary in significance. At the extreme end of the spectrum is a hefty fine of up to €20 million (£17 million, $24 million) or 4% of annual global sales.

The GDPR is retroactive, so the new defined rules are also applicable to custom audiences or other data processing generated before May 25, 2018.

Do we (need to) have a checklist?

For agencies, this post-GDPR-implementation phase is all about compiling the do's and don'ts.

And while advertisers hold the responsibility for compliance and need to design different T&C's, they will most likely pass the actual field-work to their agency reps.

If you're tracking consumer behavior or refining targeting, you will always need a solid legal basis, meaning that you need to have obtained explicit consent from the user. This is more than just mentioning the GDPR compliance in the terms & conditions. Take into account:

- Users must know what data will be collected and how it will be used
- The request for consent must be stated in an understandable language
- Consent requires action, so pre-tick boxes or inactivity don't count as consent
- Customers must be given a free and genuine choice to accept or reject
- Withdrawing consent should be possible in any case

As some of the most innovative advertising methodologies rely on customer data, a few formats are slightly different since the GDPR lift-off, which requires continuous monitoring.

Facebook & Instagram

Agencies are still able to make use of all targeting features. However, the facilitated opt-out procedures are likely to have an impact on the size of the inventory and interest groups in the short term. Most of the time Facebook will act as a data controller, meaning the platform is responsible for ensuring its own GDPR compliance. However, in some cases it processes data on behalf of the advertiser, so here are a few format requirements to double-check:

	Data controller	Data processor	GDPR compliance	What's important to know
Custom Audiences	Advertiser	Facebook	Advertiser	Facebook will process data solely on behalf of advertiser, the advertiser needs to ensure a legal basis (this can be: obtain consent, contractual necessity or legitimate interests)
Lead Ads	Advertiser Facebook	Facebook	Advertiser Facebook	Both the advertiser and Facebook are controller and processor, meaning they're both responsible for requiring user consent. The advertiser can update his T&C's to obtain user consent in real-time. Before creation of the ad the advertiser must also explicitly ad Facebook's Lead Ad terms and has the option to add additional disclaimers and checkboxes
Facebook Pixel	Advertiser	Facebook	Advertiser	The advertiser needs to ensure a legal basis (this can be: obtain consent, contractual necessity or legitimate interests)
Analytics & Measurement	Advertiser	Facebook	Advertiser	When processing offline conversions data to provide measurement or analytics reports, the advertiser needs to ensure a legal basis for processing this data

Twitter

In a way that is comparable to Facebook's approach to the GDPR, Twitter updated its Privacy Shield framework, Master Services Agreement and composed a DPA, which advertisers should review. In general, Twitter is the controller of the data they use for ad services and data derived from activity on the platform. While in some instances, Twitter processes data on behalf of the advertiser, who needs to have an adequate legal basis when deploying:

	Data controller	Data processor	GDPR compliance	What's important to know
Tailored Audience Program	Advertiser	Twitter	Advertiser	Twitter will process data solely on behalf of advertiser, while the advertiser needs to ensure a legal basis as described in Twitter's Tailored Audience Program T&Cs
Twitter Pixel	Advertiser	Twitter	Advertiser	Twitter requires advertisers to have notice and consent mechanisms in place in connection with their use of this program, as described in Twitter's Conversion Tracking Program T&Cs

https://gdpr.twitter.com

Snapchat

Snap has been claiming that its policy is aligned with the principles of the GDPR for a long time. In the run up to May 25, the company has been making further changes to give users more control over the information they share with advertisers. Snapchat is also following the likes of Facebook and Google by allowing users to opt-in or out of certain high-level audience segments in areas of the app (e.g. Publisher hub Discover).

The company has improved the age-verification efficacy of the application, by requiring parental consent and changing its data retention policy for under-16s within the EU. Users under the age of 16 will still be able to use features such as Snap Map or geofilters, but their location data will not be stored any longer.

	Data controller	Data processor	GDPR compliance	What's important to know
Snap Audience Match (SAM) Audiences	Advertiser	Snapchat	Advertiser	Snapchat will process data solely on behalf of advertiser, while the advertiser needs to ensure a legal basis as described in the Snap Audience Terms
Snap Pixel	Advertiser	Snapchat	Advertiser	Snapchat will process data solely on behalf of advertiser, while the advertiser needs to ensure a legal basis as described in Snapchat's Conversion Terms

https://businesshelp.snapchat.com/en-US/article/gdpr

LinkedIn

As the social network that stores - possibly - the largest volume of personal data, LinkedIn has implemented some drastic measurements for both users and advertisers. LinkedIn members get a lot more control over third party advertising use of their personal data (e.g. defaulted privacy settings).

The platform will also delete personal data stored in advertisers' Campaign Managers if not used or inactive for 90 days (E.g. Lead Gen Forms). Interesting to know:

	Data controller	Data processor	GDPR compliance	What's important to know
Lead Gen Forms	Advertiser	LinkedIn	Advertiser	Advertisers are required to include custom privacy policy text when creating their new Lead Gen Forms. Advertisers automatically see a required opt-in added to their Lead Gen Forms. Linkedin Members will be able to see an opt-in checkbox.
Sponsored InMail	LinkedIn	LinkedIn	LinkedIn	In many cases, advertisers will not need to take any additional action to use Sponsored InMail. However, if advertisers are providing personal data to LinkedIn to target Sponsored InMails, a legal basis should be ensured
Insight Tag	Advertiser	LinkedIn	Advertiser	Advertisers who make use of LinkedIn's Insight Tag need to ensure a legal basis and preferably consult the network's development protocol
Matched Audiences	Advertiser	LinkedIn	Advertiser	Advertisers are responsible for compliance and should ensure they have a legal basis and right to provide LinkedIn any personal data (including hashed email form) for advertising purposes. Advertisers are also responsible for the content of their ads, including GDPR compliance for any personal data contained in the ad, and any personal data that they may gather in response to their ads

Ongoing process

So, to wrap up: there's no real conclusion because the GDPR compliance will be an evolving issue. Agencies need to do what all major platforms recommend: reach out to a local counsel and ensure that we have solid guarantees on waterproof privacy policy agreements.

In the end everyone involved in the marketing loop will benefit from rigid data protection.

And even though audience sizes might shrink in the short-term because of the increased promotion of the right to erasure, the quality of this audience will ultimately improve in the long run. Just for now we can predict at least one thing: active opt-in's will be the agency's new best friend.