**A Marketer’s Guide To GDPR**

*by* [**Allison Schiff**](https://adexchanger.com/author/allison-schiff/)*// Tuesday, October 31st, 2017 – 6:00 am*

Share:

The EU’s General Data Protection Regulation (GDPR) is a looming reality set to take effect on May 25, 2018 – and the digital advertising industry is just starting to get woke.

But misconceptions about the regulation are pervasive. And despite the substantial amount of work that companies need to do in order to prepare for and comply with GDPR, many are still dragging their feet.

“I’ve heard so many things over the last six months that have just made me want to slap my forehead,” said Todd Ruback, chief privacy officer at Evidon, a provider of digital data governance solutions.

As the clock ticks down, here’s a quick and dirty guide to the most significant piece of European privacy regulation in two decades. There’s a lot to do.

**What Is GDPR?**

GDPR was adopted in April 2016 by the European Parliament and the European Council after more than four years of negotiations to give EU citizens more control over their personal data and make companies that collect, process and store personal data far more liable, especially for data breaches.

Starting in May, companies will no longer be allowed to collect or process a European citizen’s consumer data without identifying their legal basis for doing so, like, for example, obtaining freely given and “unambiguous” consent. Companies will also be barred from using previously collected data if wasn’t brought on board with the appropriate notice and consent measures.

The regulation came about as a way to harmonize and modernize privacy protection laws across the 28 EU member states and the European Economic Area. GDPR replaces the Data Protection Directive, which was formalized in 1995. Previously, under the 1995 Directive, each member state set its own data protection rules, which created an inconsistent regulatory environment and compliance headaches for companies trying to do business in the EU.

Most of what’s enshrined within GDPR isn’t actually new and carries over ideas that were already on the books in the Data Protection Directive. But GDPR does introduce several new concepts, including substantial fines for noncompliance and enhanced rights for data subjects, which are a very big deal for any company doing business in the EU or any company housing an EU’s citizen’s personal data in its database.

**What’s New In GDPR?**

**Personal data**: Treat personally identifiable data like kryptonite under GDPR.

The previous privacy regime defined personal data as name, picture, email address, phone number, physical address or personal ID numbers, like a bank account number or social security number.

But GDPR broadens the definition to include “identified” and “identifiable” data. That means personal data is now any information that could be used to identify a person, including location data, mobile device IDs and, in some cases, IP address. (Biometric and genetic data is considered to be “sensitive personal data.”)

Pseudonymous data, which is personal data that’s been hashed, encrypted or anonymized in some way using a technological method, is a potential compliance tripwire. Data that can be re-identified with reasonable effort by combining it with additional data points is also considered personal data.

**Individual rights**: The previous Data Protection Directive already gave EU citizens the right to ask a company to delete their data if it's being processed unlawfully or is no longer needed for its original purpose.

GDPR expands the right of erasure, also known as the right to be forgotten, by requiring data controllers to take reasonable steps to ensure that the data is also deleted by any third parties it’s been shared with.

Data subjects will also have the right to data portability between online platforms; the right to not be subjected to automated data processing, such as profiling; and the right to obtain a copy of their processed personal data for free and in electronic form upon request, including where it’s being used and for what purpose.

**Record-keeping requirements**: Data controllers and any subcontractors must maintain written records of their data processing activities, including why they’re processing the data and how long they plan to keep it. This information must be made available to data protection authorities upon request.

**Accountability principle**: Although GDPR doesn’t address accountability in practical detail, data controllers must clearly document all of the actions they’re taking to comply. GDPR calls this “data protection by design and by default.” If regulators ask for proof of compliance, companies must be able to easily supply it.

**Data protection officer (DPO)**: Organizations whose core activities involve systematic data monitoring or processing of people on a large-scale – like hospitals, insurance companies and banks – must appoint a DPO. How broadly "systematic monitoring or processing” will be interpreted under the law remains an open question.

The DPO is meant to help companies comply with GDPR, reporting directly to the C-suite while remaining fully autonomous. Some ad industry insiders believe having a DPO is also a show of good faith that may keep the regulators at bay.

**Bigger fines**: GDPR infractions come with significant penalties of up to 20 million euros or 4% of global annual turnover for the previous year, whichever is greater – per violation.

Supervisory authorities can consider mitigating factors when setting a fine. A company that makes an effort to comply and reports any violation as soon as possible will likely be punished less harshly than willful violations.

Regardless, the possible size of these fines could mean curtains for smaller companies, and “there’s no small irony in that,” Ruback said.

“Either they’ll go out of business, or they’ll get gobbled up,” he said. “We’ll end up with a cleaner ecosystem but also less competition. Facebook and Google, which are under so much scrutiny by the European Commission, [could actually win by accident](https://adexchanger.com/data-driven-thinking/eus-general-data-protection-regulation-favor-digital-ad-giants/).”

**Data Controller vs. Data Processor**

GDPR establishes different rules for data controllers and data processors.

Data controllers determine why and how personal data may be processed, and are required to establish a legal basis for processing data. The law states that data processors “process personal data on behalf of the controllers.”

Processors must do their processing legally and responsibly, and controllers must ensure that their processors are doing a proper job.

Although the rules governing controllers are more stringent, both controllers and processors are on the hook under GDPR. Unlike the previous privacy regime, processors are subject to enforcement actions and could be liable for big penalties if they don’t comply.

It’s unclear, however, if ad tech companies will be considered controllers or processors. The moment ad tech players start gathering insights from data to benefit other clients, even in the aggregate, they’ve possibly crossed the line into controller territory and the compliance burden could become heavier.

**Lawful Grounds**

Companies can process data if they have a legal basis for doing so. Insurance companies, for instance, have to process customer data in order to carry out the terms of a contract. Banks have to process data to comply with the law.

But there are two legal bases that marketers should know: legitimate interest and consent.

**Legitimate Interest**

Companies that are able to demonstrate a “legitimate interest” can in certain cases lawfully process personal data without consent: if the data was collected legally, if there is a justifiable reason for its use and if the processing was done responsibly.

Establishing legitimate interest requires the data controller to conduct an exercise called the “balancing test,” in which it weighs its own interests against the rights of the data subject, including the individual’s reasonable expectations about how his or her data is processed and whether the controller has the right safeguards in place.

Examples of legitimate interest include crime prevention, fraud detection, cybersecurity, conducting employee background checks and the like. “Direct marketing” is also specifically called out within GDPR as a legitimate use of personal data, but with certain caveats.

Personalized communications, targeted advertising, aggregating analytics to create trend reports and track ad performance, post-click tracking and audience measurement are all potentially okay under GDPR, as long as the controller ensures that users can easily opt out at any time.

What’s unclear is whether companies engaging in online behavioral advertising and programmatic advertising can claim legitimate interest. It’s unlikely, said Johnny Ryan, head of ecosystem at PageFair.

“Some ad tech companies seem to have convinced themselves that they’re covered by legitimate interest, but you can’t use legitimate interest to justify all of the crazy stuff that happens in RTB,” he said. “Anyone who knows what they’re talking about will admit that, at least in private.”

**Consent**

Consent has always been a cornerstone of European privacy law, but GDPR raises the bar considerably.

Data controllers – the parties that decide how personal data is used – must get “unambiguous” consent for each purpose they plan to use the data for. In other words, a company can’t get consent to do one thing and then turn around and use that data for something else.

Consent must be freely given and specific.

Opt-out models (aka pre-checked boxes) will not fly. Neither will what’s known as an informed consent model, which is when a site loads tracking cookies at the same time as the page loads along with a brief notice, usually in pop-up form, alerting the visitor that the site uses cookies. Barrier pages, where content is blocked until a user agrees to enable tracking, won’t work either.

The bottom line is that a consumer’s action must be both affirmative and informed. The data protection authorities in the UK, France and Germany all agree that consumers can signal consent to processing by ticking a box on a website, but only if they’ve been shown a clear notice with straightforward language beforehand.

Ad tech and martech vendors generally don’t have a direct relationship with consumers, so obtaining consent for tracking or data collection is a tricky proposition. They’ll most likely have to rely on consumer-facing entities like publishers and marketers to get consent on their behalf.

Evidon is taking a different tack [via](https://adexchanger.com/privacy/evidon-launches-consent-platform-clock-ticks-gdpr/) a universal consent platform for GDPR compliance that claims to provide consumers with an ability to opt in to data collection, get visibility into what’s being collected and modify what’s being tracked.

But not everyone’s convinced that middlemen can thrive under GDPR.

“The third-party ecosystem is not going to hold up in a GDPR world,” said Mike Anderson, CTO and founder of Tealium. “GDPR is about first-party relationships.”

**Who’s Responsible When There’s A Problem?**

Marketers and publishers are potentially accountable for mistakes made by third parties, which means they’re about to get a heck of a lot more choosy about who they work with. GDPR therefore ups the ante on the importance of due diligence and vendor management.

And consent is not the silver bullet for GDPR compliance. Having obtained it, “you have to make sure nobody in the chain who might get data you share will misuse it and expose you to legal hazard,” Ryan said.

Yet hope springs eternal among marketers and ad tech companies that largely seem to be burying their heads in the sand on the accountability issue.

“The fact is: If something goes wrong, they all get in trouble,” said Melissa Parrish, VP and research director at Forrester. “There is no provision for passing the buck.”

**Inconsistencies With ePrivacy**

Although GDPR gets all the headlines, ePrivacy, aka the Cookie Directive, is potentially more impactful for marketers. In broad strokes, GDPR deals with the handling of personal data, and ePrivacy covers privacy as it relates to electronic communications.

If you’ve visited a European website and been served a pop-up banner warning you that “by visiting this site, you accept the use of cookies,” then you’ve experienced ePrivacy in action.

That’s been the norm since 2002, when the directive was passed. But soon basic cookie notices aren’t going to cut it.

European regulators are updating ePrivacy to make it more consistent with GDPR and simplify cookie compliance, which has devolved into a deluge of consent requests. Regulators hope to finalize ePrivacy and bring it into force by May to coincide with the official rollout of GDPR.

However, if both ePrivacy and GDPR include statutes to handle the same situation, then the ePrivacy rules prevail. And therein lies the rub: The ePrivacy draft currently under review doesn’t include legitimate interest as a legal basis for processing, which leaves consent as the only likely legal basis for marketers processing data come May. (The performance of a contract could possibly work as a legal basis in certain situations.)

It’s highly unlikely that the revamped ePrivacy rules will be approved by May – it took four years to pass GDPR, and the ePrivacy draft has only been under review since January – and that’s creating uncertainty.

“Right now, ePrivacy doesn’t harmonize with GDPR, so we have a gap,” said Sheila Colclasure, Acxiom’s global chief privacy officer. “We need to make sure that the Cookie Law allows for legitimate interest and doesn’t disrupt innovation, but there’s still a gray area in terms of how ePrivacy is going to work and how Europe will operate under the ePrivacy Directive if the ePrivacy Regulation doesn’t come into force when GDPR does.”

Either way, if the ePrivacy regs don’t include legitimate interest, “that’s bad news for ad tech companies,” said Omer Tene, VP of research and education at the International Association of Privacy Professionals.

“Unless there ends up being a legitimate interest revision in there, it’s hard to see how ad tech players can conceivably comply with the ePrivacy regulations,” Tene said. “This is something it’s extremely important for advertising intermediaries to be attentive to.”

Especially considering the potential penalty for noncompliance. The fines laid out in the draft ePrivacy regs hew closely to those within GDPR: up to 20 million euros or 4% of global annual turnover.

**GDPR Misconceptions**

At the top of the list of wrongheaded GDPR ideas: Companies that aren’t in Europe don’t have to worry about GDPR.

Not true. GDPR has jurisdiction over the personal data of EU citizens, regardless of where it’s processed.

“GDPR may have been born in the EU, but it applies to any company in the world that targets its services at a European audience, that collects personal data in a meaningful way or that regularly monitors information about Europeans,” Tene said. “That’s a big change compared to the previous regime, where you had to be present on the ground in order to be subject to a data protection directive.”

Regardless, a lot of smaller and midsize ad tech and martech companies seem to be taking a wait-and-see approach to GDPR – and it’s not a smart move, Evidon’s Ruback said.

“They’re not being proactive, and that’s a bad business strategy, especially when publishers and brands are already having conversations with their digital supply chains and modifying their agreements to indemnify themselves in case they’re penalized due to the third party’s transgression,” Ruback said.

But companies are starting to get the hint. According to a joint annual governance report released by the International Association of Privacy Professionals and Ernst & Young in October, 95% of respondents – 75% of which are located outside of the EU – believe that GDPR applies to them, and 50% of US firms say GDPR compliance is driving their privacy program.

**Privacy Shield**

The Privacy Shield is the EU-US data transfer agreement that replaced Safe Harbor. It passed its first annual review in mid-October, which means European officials believe it provides an adequate level of cross-border data protection. Self-certifying under Privacy Shield before May 2018 is one way for US companies to ensure they have a valid mechanism to transfer personal data between the EU and the US.

By the same token, Privacy Shield only applies to international data transfers and doesn’t ensure compliance with other key tenets of GDPR, including obtaining consent, conducting privacy impact assessments and appointing a data protection officer, among other provisions.

**Checklist**

The GDPR is a sprawling piece of legislation with 99 dense articles, and there’s no easy list of things to do to ensure compliance. It’s best to tackle the easier stuff first before taking on the thorniest aspects.

“All a regulator needs is a browser, a laptop and a list of websites to see who’s being transparent,” Ruback said. “Do you have a consumer-centric and easy way to communicate your data practices and give individuals control over their personal data? That’s the regulators’ low-hanging fruit and something they’re more likely to enforce before they start digging into a company’s internal processes and honoring things like the right to be forgotten."

**Determine whether your company is a controller or a processor.** The distinction will have an impact on how you approach compliance.

**Conduct a data protection impact assessment (DPIA)**: Run a risk analysis of your data process. The first step is to map your data flows and get a clear understanding of where you’re collecting data from, who you’re sharing it with, if there’s the potential for data leakage and how you maintain, retain and protect data when you have it. A DPIA helps companies figure out if they’re in compliance with GDPR and/or how much work they’ve still got to do to get there.

**Take a look at your contracts**: Review your supply chain to determine whether your agreements with partners are up to date and include GDPR-related clauses – for example, what to do in case of a breach or an enforcement action. This can be part of the DPIA process.

**Do you need a DPO?** Whether a company is required to appoint a data protection officer depends on the scope and scale at which it tracks data subjects. The law says “regular and systematic monitoring … on a large scale.” But having a DPO is always better than not having one.

**Documentation**: Controllers are required to document that the processing of data being done on their behalf is up to the GDPR’s standards, including the creation of internal policies on opt-ins, data retention and management. If a Data Protection Authority comes knocking, you need written proof of your procedures at hand.