DIGIDAY

# THE DIGIDAY GUIDE TO GDPR

The European Union's new General Data Protection Regulation is a horribly complex maze of information. It's fair to say that plowing through unspeakably dry legal documents for hours on end is a niche pastime that very few enjoy. Nevertheless, the GDPR will have long-lasting effects on how all companies collect and use data to sell products or services in Europe or use it for advertising and analytics purposes.

---

Here's Digiday's primer on all you need to know.

# TABLE OF CONTENTS

# WTF IS GDPR?

The GDPR is legislation that replaces the current out-of-date law and aims to give individuals more control over their personal data, by requiring that businesses gain more explicit consent from them to collect and use it.

## OK, WHY IS IT IMPORTANT?

It will unify data privacy laws across Europe, and regulate the collection, use and sharing of online identifiers like cookies and advertising IDs that brand advertisers, agencies and third-party data partners, e-commerce companies and media owners use in digital advertising and direct marketing. In a nutshell, that means any company, whether a retailer, publisher or ad tech company, must gain (or regain) approval to use audience and customer data.

## I KEEP HEARING ABOUT EPRIVACY REGULATION.

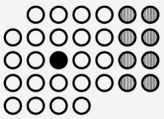
A new ePrivacy law is being devised. Although it's a separate law than the GDPR, it's hard to talk about one without the other. The main difference between the two: ePrivacy relates solely to the collection and storage of cookies. The GDPR is far broader. Unlike the GDPR, the ePrivacy law is still in draft mode, so it has yet to be voted on and enforced. So there's a lot of gray areas still.

## WHY IS THAT IMPORTANT?

It will free European Union countries from having to run annoying on-site banners that ask visitors for consent to use cookies for tracking. Instead, website users will have to specify their consent settings within their browser settings, essentially making browsers the gatekeepers, and behavioral advertising will be directly affected.

# GDPR BY THE NUMBERS

## MAY 25, 2018



Deadline for GDPR compliance.

**70** or so of the GDPR requirements can be interpreted locally by each of the EU's **28** different states.

Maximum fine for noncompliance

## €20 MILLION

## (£17 MILLION OR $24 MILLION)

or 4 percent of annual global sales (whichever is greater)

## 72 HOURS

The amount of time a company has to report a data leak. Here's looking at you, Yahoo and Equifax …

# WHAT MARKETERS NEED TO KNOW

| | |
|---|---|
| **Do** | Take the time to understand how data is gathered, stored and shared within your business. You can't prepare for the regulation as a marketer until you know the state of your own assets. |
| **Do** | Make changes to existing contracts between your advertising partners. You need toclearly set out contractual liabilities and obligations to each other, including who has the obligation to obtain consent. |
| **Do** | Work out how to communicate the GDPR. Marketers need to spend more time thinking about how they can offer a value exchange with their customers that makes sharing data feel natural and meaningful. |
| ***Don't*** | Think that by being based outside of Europe you can dodge the regulation. If you have collected data directly or indirectly from EU citizens, then you are still liable for a breach and could be slapped with a hefty fine. |
| ***Don't*** | Believe consent is the panacea to preparing for the GDPR. If personal data is passed into the online bidding system, then you have exposed the brand to risk because you have no control over where that data ends up. |
| ***Don't*** | Think processing data under "legitimate interests" is a "get out of jail free card" that could be used to legally market to anyone without consent. The "legitimate interests" of an advertiser to process personal data must be balanced against the rights of the consumer. |

# WHAT PUBLISHERS NEED TO KNOW

| | |
|---|---|
| **Do** | Find out how third-party tech partners in your supply chain are using and sharing data, as they'll also need to be compliant. |
| **Do** | Appoint a data protection officer that will help establish a compliance map, or think about outsourcing a DPO. |
| **Do** | Figure out how best to communicate to audiences why you'll need to be in contact for explicit consent and what the value exchange will be for them in a digestible, creative way. |
| ***Don't*** | Sit back and wait for the Information Commissioner's Office to give more detail around consent guidance. There is plenty to be working on. |
| ***Don't*** | Assume that your existing privacy notices, implicit consent notices and pre-ticked cookie consent boxes will be sufficient under the GDPR. Companies will now have to create information opt-ins that require positive user action that is separate from standard privacy notices. Plus, these notices must be in simple language, devoid of legalese, so that the average individual will be able to understand what is happening to their data. |
| ***Don't*** | Think that just because you have a privacy notice on your website that nothing needs to be present on your mobile app. Companies should make sure that a privacy notice is present in the description of the app prior to it being downloaded. Additionally, once the app is downloaded, the privacy information should be accessible and never more than "two taps" away from the current page. |

# WHAT TECHNOLOGY COMPANIES NEED TO KNOW

**Do** Prepare to educate people about who you are and what you do. The GDPR requires companies to list who they are sharing their data with, which means much of the public will be learning about you for the first time. They'll be unsure of and hesitant about why so many companies suddenly have access to their data.

**Do** Work with a chief data officer either in-house or externally to review your contracts and obligations under the GDPR. Data processors are held to the same standards as controllers under the GDPR regarding things like data security, transparency and providing users access to review their data. Furthermore, there are gray areas in which data processors can be considered data controllers when working with subprocessors. The more proactive you can prove you've been at investigating and documenting your efforts to clarify this, the better.

**Do** Determine the legal basis for which you are collecting and processing data. There are six different types of legal basis, all of equal status, such as consent or legitimate business interests. However, once you declare your legal basis, you will be unable to change it without first notifying all of your consumers and providing them the means to alter or remove their data, in accordance with their fundamental human rights under the GDPR.

***Don't*** Assume you will be able to hold on to consumers' data forever. The GDPR mandates that data controllers and processors state their purpose for collecting user data and the duration they will retain it. Vendors will not be able to use vague terms to prolong the length of time before they must erase data.

***Don't*** Believe that just because it is difficult to provide someone with their personal data that it is impossible by GDPR standards. While pseudonymous data is likely exempt, vendors and all companies have a responsibility to allow people to edit, erase and restrict the use of any identifiable user information.

# GDPR GLOSSARY

- **Data controllers:** Whomever the data source is, so website owners.

- **Data processors:** Companies or organizations that process data that comes from an external source. External sources could be publishers.

- **DPIA:** Data protection impact assessment. Tests run when implementing new technologies to ensure that any data processing meets "individuals' expectations of privacy."

- **Explicit consent:** This must be freely given by the consumer, after the company wishing to use their data has informed them of the exact purpose for its use.

- **Lawful basis:** The legal justification to explain under what necessistation companies collect and process personal data. Currently there are six different types of lawful basis ranging from consent, contract, legal obligation, vital interests, public task, legitimate interest.
  - **Consent:** When an individual gives a business positive affirmation to collect their data
  - **Contract:** When processing is required to fulfill an agreement between a business and a consumer
  - **Legal obligation:** When collection and processing is required to comply with the law (does not include contractual obligations)
  - **Vital interests:** When collection and processing is required to protect someone's life
  - **Public task:** When collection and processing is necessary for a public service or interest
  - **Legitimate interest:** When a business can prove it has a justifiable reason for using customer data, which can include "for business purposes."

- **Personal data:** Any data, like location data, that enables an individual to be personally identified.

- **Privacy by design:** Ensuring privacy and data protection compliance is baked in at the start of any project, not as a bolt-on. This will be a new form of best practice.

# GDPR GLOSSARY

- **Pseudonymous data:** The processing of personal data in such a way that the data can no longer be attributed to an identified or identifiable individual. Any additional information that can identify an individual must be held separately and securely from processed data to ensure it can't be attributed to the individual.

- **Right of access:** Ability of consumers to get companies to acknowledge if their personal data is being processed, and to access that data. Both free of charge.

- **Right of erasure:** Also known as "the right to be forgotten", allows an individual to request a company to delete their personal data under certain conditions, or if the individual withdraws their consent

- **Sensitive Personal Data:** Personally identifiable data unique to a specific individual pertaining to health, racial, and ethnic information.


DIGIDAY
HOT
TOPIC
GDPR
London
May 1, 2018
A one-day event exploring everything you need to know about a post-GDPR world
Save 10% with code
GDPRGUIDE
Learn more at digiday.com/events

# COMMON GDPR MYTHS, DEBUNKED

***Myth*** The biggest threat is eye-watering fines.

**Reality** While it's true that companies that don't comply with the new laws will face fines of up to 4 percent of their revenues or a maximum €20 million (£17 million or $24 million), these kinds of fines will be rare. The Information Commissioner's Office has said it prefers the carrot to the stick in this case, though there will be other forms of punishment for not complying.

***Myth*** The GDPR is a Europe-only issue.

**Reality** Far from being some typically bureaucratic issue that applies to the 28 members of the EU (including the U.K., as Brexit won't affect its compliance), the GDPR will affect any company that offers goods or services to consumers in the EU or monitors the behavior of people located in Europe, regardless of where their offices or ad servers are based.

***Myth*** Data privacy notices and opt-ins have to be done exclusively online in the form of written statements.

**Reality** Companies are not restricted to online written statements. In fact, the ICO discourages this, especially when presenting information to hearing- or visually impaired individuals. The GDPR and the ICO give companies the freedom to present the required information in a multitude of ways, including videos, infographics, handwritten forms, audio recordings and more.

***Myth*** When relying on consent to process personal data, consent must be explicit.

**Reality** Explicit consent is required only for processing sensitive personal data. For non-sensitive data, a person's consent can be unambiguous and implied.

***Myth*** Everyone needs a data protection officer.

**Reality** Unless you're a public authority, an organization that performs large-scale tracking or a business that processes vast amounts of sensitive personal data, then you don't need to hire a DPO. Appointing one, however, is encouraged by regulators in the interests of best practice.

# DIGIDAY RESEARCH: GDPR WILL BENEFIT THE DIGITAL MEDIA INDUSTRY

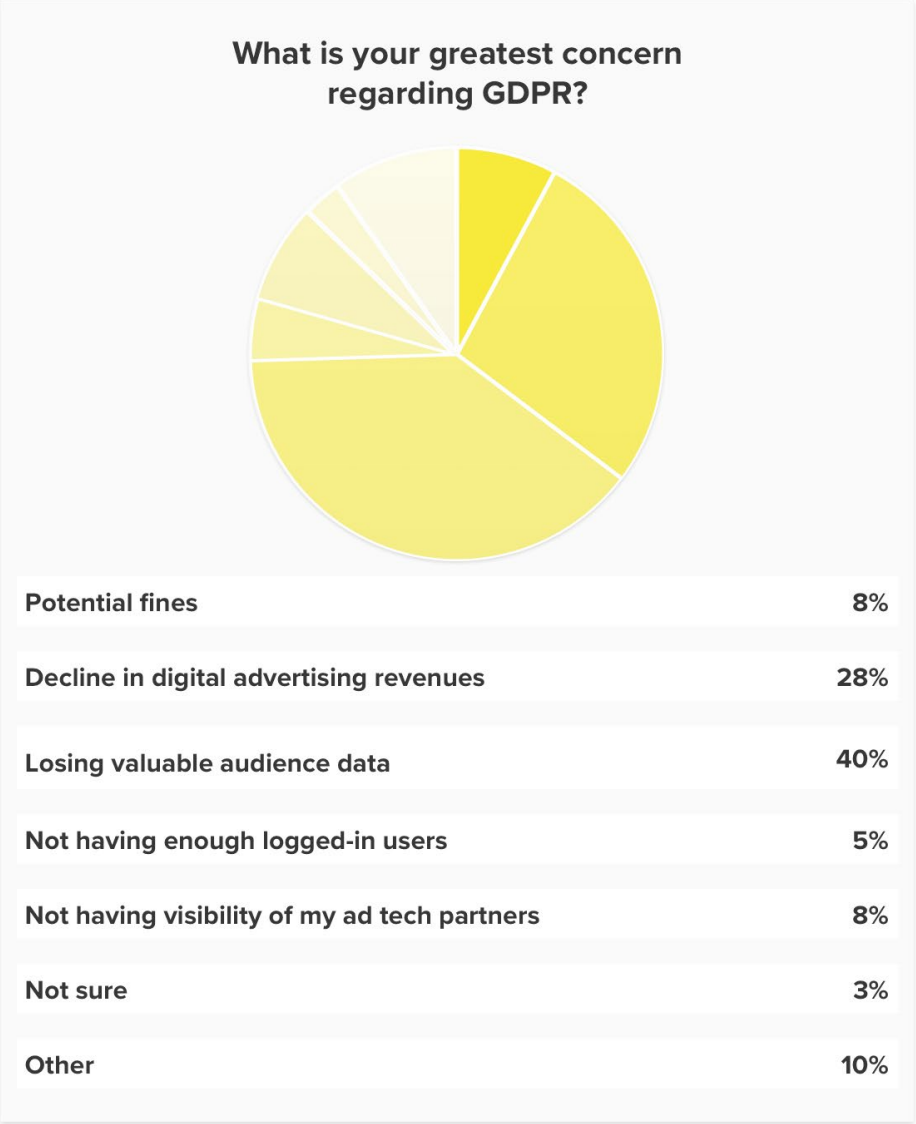
There's still a lot up in the air when it comes to the GDPR. In this sneak peek from exclusive research, available to Digiday+ members, we surveyed publishers about what they expect from the coming regulation. To get more research like this, become a member of Digiday+.

Despite the critics, the GDPR benefits the digital media industry. Digital advertising is rife with shady practices and inaccurate data that proper GDPR enforcement could reduce. In a survey of over 20 media and ad tech company executives at the Digiday Hot Topic UK: Data-Driven Publishing last November in London, Digiday found that people are warming to certain aspects of the GDPR. Nearly half of all respondents expect the GDPR to help improve the quality of data that advertisers collect, while none thought it would damage future data quality.


Fifty-three percent of respondents think data quality won't change, but that less will be collected as users become more adept at opting out of tracking technologies. The potential drop in first-party data doesn't necessarily mean that marketers will suddenly rush to prop up campaigns with third-party data from vendors and data management platforms. Why? Because almost all marketers hate third-party data to begin with.

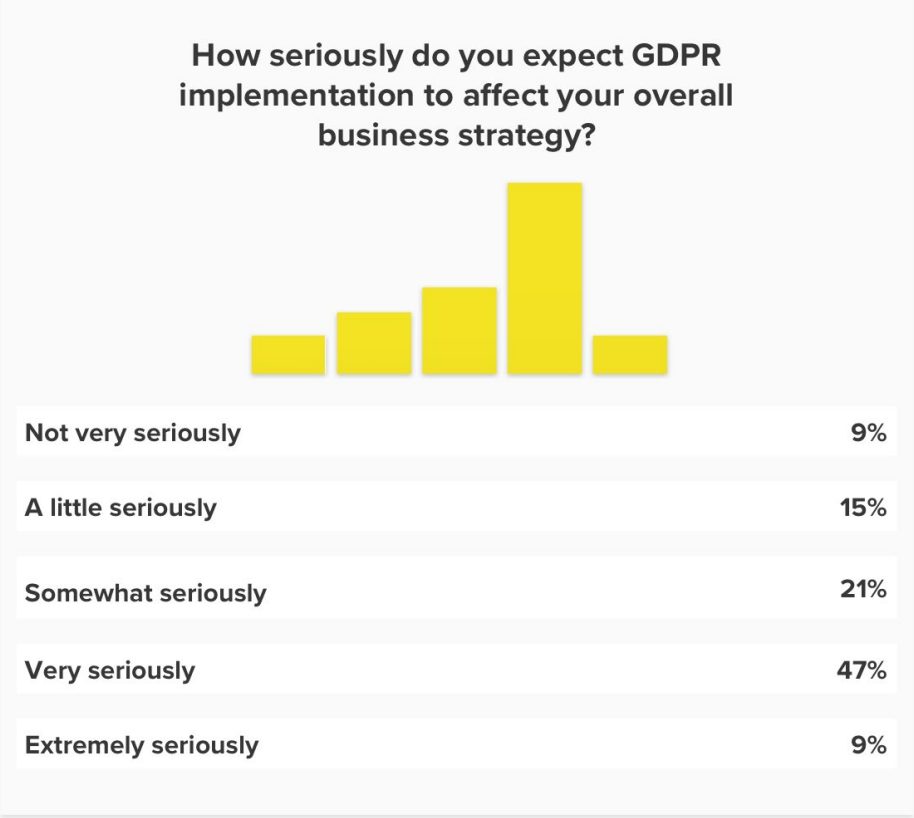
More than 80 percent of people believe third-party data is unreliable. Earlier Digiday research on the GDPR found that publishers were most concerned about losing audience data as a result of the legislation. Instead of going back to data vendors, which the GDPR will significantly affect, marketers are already exploring other alternatives.

Potential fines pale in comparison to fears about losing audience data and digital revenues for people reacting to the GDPR. Respondents were five times more likely to be concerned about a loss of audience data than about being fined. Under upcoming GDPR regulations, EU consumers will not be obligated to share their personal information with sites they visit. A recent report by PageFair found that only 23 percent of marketers expect consumers to disclose their data for advertising purposes.




Publishers' fear of the GDPR should be expected because the new laws will redefine the online relationship between companies and consumers. Fifty-six percent of publishers think the GDPR will have a very serious or extremely serious impact on their overall business strategies. This figure jumps to 80 percent for European publishers. No non-European publishers anticipate the GDPR having a very or extremely serious impact on their business strategies.

Publishers' fear of the GDPR should be expected because the new laws will redefine the online relationship between companies and consumers. Fifty-six percent of publishers think the GDPR will have a very serious or extremely serious impact on their overall business strategies. This figure jumps to 80 percent for European publishers. No non-European publishers anticipate the GDPR having a very or extremely serious impact on their business strategies.




The EU represents a growing digital marketplace with 500 million citizens. European digital ad spend continues year-over-year growth, totaling $49.8 billion in 2016. Depending on how companies seek to protect themselves from GDPR noncompliance, this growth could be in jeopardy. According to some industry insiders, agencies and trading desks will likely cut back on programmatic spending because of its reliance on consumer data and greater potential exposure to GDPR penalties.

Publishers still aren't sure what the final GDPR protocols will require of them. This could explain why almost two-thirds of publishers have yet to implement their GDPR strategies. For U.K. publishers specifically, the Information Commissioner's Office recently released updates for data breach notification requirements and fine administration. However, the ICO has yet to lay out final comprehensive GDPR compliance standards.

May 25 will be the day of reckoning for media and marketing. The GDPR is creeping up, but it has the potential to be a wrecking ball -- especially in light of the confusion that has emanated from its two-year gestation period. We hope this guide went some way in clearing up that confusion.