E-BOOK

The Agency Guide to GDPR

Adzapier
The New Era of Data Privacy

Agency's Guide to GDPR

Introduction

From eCommerce stores to marketing agencies, many organizations collect and use data. As organizations of all sizes rely more on data and technology, consumers demand more transparency and want a clear understanding of their privacy rights.
If your agency is not prepared for new privacy regulations worldwide, now's an excellent time to understand the steps needed to comply with General Data Protection Regulation (GDPR) and the new privacy standards.

E.U. regulators believe that companies have been exploiting personal data for their gain and aren't transparent about using it. GDPR is here to change that and put the power back in the consumer's hands.

What is GDPR?
The General Data Protection (GDPR) came into effect on May 25, 2018. This law gives consumers more control by requiring the consent of the collection and use of their data. It standardizes a wide range of different privacy legislation across the E.U. into one central set of regulations that will protect users in all member states.

Personal data refers to any information that is related to personal identity, such as:


Picture

Name

E-mail Address

Phone Number


Social Security Number


Post in Social Media

I.P. Address


Location


Occupation


Even Social Media Updates

Introduction (continued)

The primary goal of the GDPR is to ensure privacy, security and enable people to have control over their data. Regardless of whether you operate inside the E.U., if you have online visitors from the E.U., these rules and regulations still apply to your agency and clients. Businesses need to administer privacy impact evaluations, improve the way they request permission, and document how they use personal data.

And, because it's a regulation and not a directive, it is legally binding - meaning it cannot be opted out of or ignored. Not complying could lead to fines of up to **$2.25 million or 4% of your global turnover!**

Here are a few recent examples of how high these GDPR fines can be:
- British Airways faced fines of up to $225.95 million for a data breach in September 2018.
- Marriott International was fined $20.29 million for a significant data breach that may have affected up to 339 million guests.

Simply put, the E.U. isn't taking this lightly.

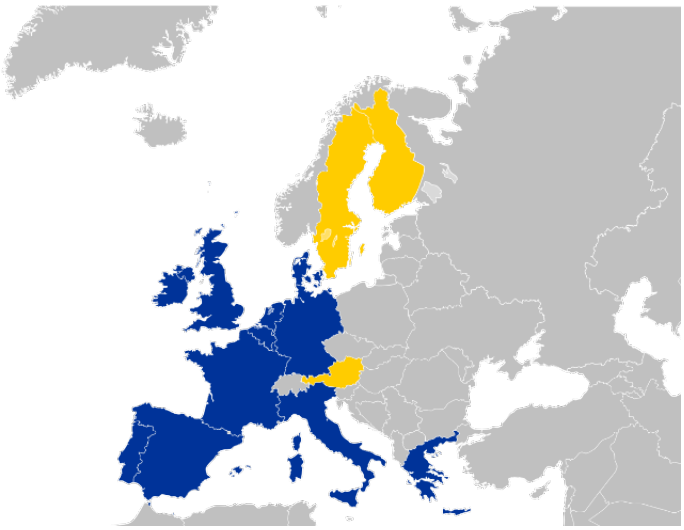
History of Data Protection

While this may seem like a relatively new development, it's worth nothing Europe has had laws covering data protection for over 40 years.

The Data Protection Directive (1995) helped define rules on information management. However, these directives were not created with the digital nature of today's business and commerce.

There were 27 national data protection regulations at the time of GDPR conception. Then on January 25, 2012, the European Commission (E.C.) announced it would create a unifying data protection law across the European Union which came to be GDPR. The E.C.'s objectives included:

- The harmonization of the 27 national data protection regulations into one unified regulation.
- The improvement of corporate data transfer rules outside of the E.U.
- The improvement of user control over personal identifying data.



A compliance date of May 25, 2018, was set to give businesses a chance to prepare for compliance, review data protection language in contracts, consider a transition to international standards, update privacy policies, and review marketing plans.

6 Steps to DSAR (continued)

GDPR is all about the consumer.
Now, marketers must gain permission from consumers before using their data. This means data-rich marketing activities like digital ads will need to rely on first-party cookies. GDPR will force marketers to give up their behavior-based data collection.

Couldn't you just require someone to agree to a Terms of Service when they sign up?
I'm afraid not. "Checking the box" isn't considered active consent. Companies that rely on behavioral data for advertising like Facebook and LinkedIn are already trying to find loopholes to get around GDPR.

Facebook routed 1.5 billion users out of reach of GDPR privacy laws.

Another part of GDPR that could cause trouble for agencies is the ban on automated decision-making (e.g., applying algorithms to personal data to create assumptions and target ads) without active consent.

What will take the place of behavioral data collection marketers have relied on for decades to channel the right marketing messages to the right people at the right time?
For many, contextual advertising will be the way forward. This is powerful because ads are shown based on their content in real-time, not on past behavior. For instance, if a Wall Street Journal reader is looking at a digital article about the hit show "Billions," he might see a contextual ad by Showtime reminding him about an upcoming season premiere. While contextual ad placement might seem more tedious than behavior-based ad placement, many marketers have used it successfully. Finding relevant content has become easier thanks to advances in A.I.

Today, natural language processing (NLP) allows for a deeper understanding of each page. Instead of "this page mentions travel to France" to "this page is about a joyful experience traveling to France." Machine learning is helping advertisers move away from keywords and whitelists and relying on A.I. to find the most relevant content.

Now, behavioral data collection will not go away entirely...yet. But it's in the works. Browsers like Firefox and Safari already banned 3rd party cookies, with Google Chrome pledging to follow suit by 2023.

How Does GDPR Affect Internal Processes?

Another Core Part of GDPR is the rights of the person including:

Right to Access
The right to know if their data is being processed and the right to access it

Right to Rectification
The right to update and keep their current data being processed and complete any incomplete data

Right to be forgotten
The right to request to have their data erased and removed under certain conditions

Right to the restriction of processing
The right to request the restriction of their data being processed under certain conditions

Right to be informed
The right to know when their data has been erased, changed, or shown, especially as a consequence of their rights listed above

Right to data portability
The right to receive their data that has been collected in a common and easily readable file format

Right to object
The right to-object and request that their data no longer be processed unless there is a compelling legal reason to do so. A person has the right not to be profiled, especially for marketing purposes

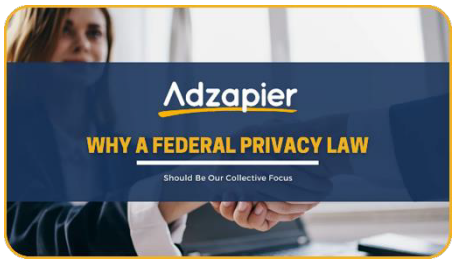
Right to not be a subject to a decision based solely on automated processing
The right to not be the subject of automated profiling.

Conclusion & Final Words

GDPR is here and is affecting agencies around the world. Understanding what GDPR means for consumers and how you can comply can improve transparency, eliminate unnecessary fines, and push your team to create more relevant content.

Get a Free Consultation

Keep reading



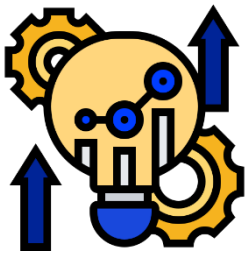
Who will be Affected by GDPR?

GDPR is considered the most extensive data privacy regulation enforced to date. It applied to anyone who stores, collects, records, organizes, and processes the personal data of E.U. citizens.

In your agency, three primary roles will have the most noticeable changes

1. Email Marketing Managers

For most marketers, emails are a stable of lead generation.
Under the GDPR, buying or scraping lists is strictly forbidden. All users must give consent to be contacted. You cannot contact them without permission. Email marketing managers will have to work closely with the rest of the team to ensure qualified leads are opting in for relevant content.



2. Marketing Automation Specialists

Every name in your automation sequence must give you permission. Marketing automation can be powerful but costly if your software sends emails on your behalf without consent. If a user opts out, they need to be removed from any current and future sequences.

3. Business Development

If you've obtained information from a list that's been scraped or bought and has E.U. citizens, your BDR's can not contact them without consent.

This will require more time spent building relationships, generating referrals, and creating expertise-building content to attract new leads.

4 Steps to GDPR Compliance

While it may sound overwhelming, there are ways to make compliance more manageable. Here are four steps that will help you ease the impact of these regulations on your organization.

Data Security

- When you begin developing a product, take data protection into account.
- Encrypt, pseudonymize, or anonymize personal data wherever possible.
- Create awareness about data protection within your team and build an internal security policy for your team members to keep everything on track.
- Always have a dedicated process to notify the authorities, and your data subjects, in case of a data breach.
- Define when your organization should conduct a data protection assessment and have a resource to process it further.

4 Steps to GDPR Compliance

Accountability and Governance

- Appoint someone responsible for enabling GDPR compliance across your organization.
- Appoint a (DPO) Data Protection Officer. If your business is outside of the E.U., ensure an appointed representative within one of the E.U. members states.
- Sign a data processing agreement between your organization and any third-party firm to process the personal data on your behalf.

Transparency

- Your published Privacy Policy should have clear information about how you process data and a clear explanation of legal justifications of this data collection.
- Have legal justification for all your data processing activities.
- Convey information that educates users on what information your organization processes and who has access to it.

Privacy Policy & Rights

- Customers should access information and have access to all data your organization collects about them.
- Customers should be able to correct and update inaccurate information.
- Customers can ask organizations to delete their data, and organizations must respond within 30 to 45 days.
- Opt-in: GDPR is privacy by default. Before an organization collects a user's data, the user's data consent must first be obtained and approved.
- Opt-out: The user can stop an organizations' use and collection of their data at any time.
- Organizations should make sure customers can easily access their data in a format that can be quickly reviewed and/or transferred.

Practical Applicartions

Now, this probably seems a bit overwhelming. You're not alone.
73% of businesses weren't ready for GDPR compliance, according to Osterman Research. In nother study, Symantec found that 23% of businesses felt they were only partly compliant by the May 2018 deadline.

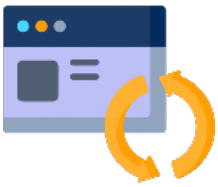
If you're still struggling with compliance, we've got a few action items to help get you started.`

Double-check your mailing list.

According to various studies, up to 75% of marketing databases are no longer compliant with GDPR. Pruning users who don't have opt-in proof can help eliminate any early problems.

Create content worth reading.

How relevant is your content to your potential customer? Create content your prospects want to read, including blogs, white papers, and eBooks can consume with opt-in.



Utilize a pop-up.

You know those annoying pop-ups you see on a new site? Here's good news, they still work. Pop-ups generally have decent click-through rates—often around 2%—higher than other kinds of ads. Pop-ups helped BitNinja increase subscriptions by 114% and boosted leads by 162%.

Have your sales team get personal.

Social selling and account-based marketing are your sales team's best friend with GDPR. Share relevant content with qualified prospects on social media to keep your pipeline full.

Try push notifications.

A push notification is a pop-up Message that appears on a desktop or mobile device. Marketers can use push notifications to send a message to subscribers at any time. But since push notifications don't collect personal data and users are required to opt-in, these are a great alternative that is still GDPR-compliant.