HOW TO MAKE YOUR WEBSITE COMPLIANT WITH THE GDPR

A 5-step process to help manage the transparency and consent requirement of the new EU legislation
WHAT IS THE GENERAL DATA PROTECTION REGULATION AND DOES IT APPLY TO ME?

The General Data Protection Regulation, or GDPR, is a massive data protection or privacy law emanating from the EU that will become the de facto national privacy law in the United States. Because of its low triggering mechanism, it will apply to most organizations, regardless of where they are located. For the law to apply, an organization merely has to offer its products or services to an EU resident, be established in the EU, or be engaged in widespread website behavioral monitoring. This last trigger, inserted into the final legislation at the last moment, is specifically aimed to sweep up the digital advertising ecosystem as a whole. This means marketers, publishers, and myriad technology companies critical to the smooth functioning of the opaque digital advertising industry must all comply.

The GDPR goes into effect on May 25, 2018. The goal of the law is simple: to give control of personal data back to the individual. While simple in theory, the law is dense and complex and of the 99 different articles in the GDPR, a full 39 require companies to document and be able to provide evidence of compliance. This is called the Accountability Obligation, and is a central theme to the law.
The GDPR requires companies to have a comprehensive understanding of all the data they collect, whether it's personal data or not, and how they use it. Specifically, companies must look at every single process and line of software code and go through a privacy impact assessment to determine if there is a privacy risk to the individual, whether she be a customer or employee. Then, for each data element collected and used, the company must determine if it has a legal basis to collect that data.

There are a number of enumerated categories, but if none of them fit – and that will most assuredly be the case for most website data collection – then the company will have to obtain valid consent directly from the individual. To make matters more complex, consent will be more difficult to get right. Under the GDPR it can’t be implied or inferred from someone’s actions.

Instead, valid consent must be specific to the data being collected, by an affirmative action that is unambiguous. Anything less will fail. This is going to rock the digital advertising industry like nothing seen before.
WHAT IS THE RISK OF NON-COMPLIANCE AND WILL THE GDPR BE ENFORCED?

The GDPR has real teeth to it. Penalties and fines can be as high as 4% of annual revenue or €20 million, whichever is greater. Furthermore, for the first time, class action litigation is also allowed, resulting in exposure to both regulatory enforcement and private litigation for the same transgression. We can anticipate robust enforcement from the data protection authorities, and they have been kind enough to signal that their priority enforcement actions will focus on transparency—how openly and honestly a company communicates its data practices—and whether they obtain valid consent, especially for the ubiquitous website data collection occurring on all websites.
A DAUNTING TASK, BUT THERE’S A WAY FORWARD

It’s no surprise that managing compliance with the transparency and consent requirement of the GDPR presents a daunting undertaking.

Yet companies need to become compliant, and quickly. How to get there, especially when it comes to obtaining consumer consent, is a question many seem to be saving for the last minute.

A Q1 2017 survey by the U.K.’s Direct Marketing Association found a revealing level of unpreparedness:

- 26% of U.K. marketers admitted they were unprepared for GDPR.
- 1 in 5 U.K. B2B marketers had no plan in place for compliance.
- 71% said obtaining consent was their biggest compliance concern.
- By comparison, a survey of U.S. multinationals found 92% considered GDPR compliance a top priority, with 77% planning to spend $1 MM+ on it.

In this guide, we’ll explore the various challenges involved in becoming compliant with the GDPR consent requirements, which need to be swiftly addressed by privacy/compliance officers, data protection managers, corporate legal departments and other stakeholders.

We’ll also show how there’s a solution at hand for website data collection, by laying out a step-by-step process for achieving compliance with the GDPR consent requirements. Plus, we’ll explain how following it can actually create a competitive advantage for companies as they improve data processes, digital governance and customer experiences, leading to increased consumer trust.
A GDPR ROADMAP: 5 STEPS TO WEBSITE COMPLIANCE

GDPR represents a sea change in how businesses handle and interact with consumer data.

Here are the key steps to achieving compliance with the GDPR transparency and consent requirements by May 2018:

1. Map your Digital Supply Chain

Even a closely-managed site may have an increasing number of tags from third-party vendors embedded on its pages, enabling their various digital marketing tools to function.

Often, these tags may give data access to other outside firms that the website operator isn't aware of. By permitting those tags on its site, a company is implicitly giving those vendors the right to collect visitor data.

One recent survey found that the top thousand most-visited U.S. websites had an average of 75 technologies in their marketing cloud.3

Under the GDPR, you are responsible for providing notice and obtaining consent for each one of these technologies, even those you have not knowingly authorized. That means:

- You need to conduct a thorough audit of your website to gain a panoramic view of your “digital marketing supply chain” of third party vendors.

- You will need to work with both marketing and IT to get greater visibility into your digital marketing apparatus. That transparency is among the many mandates GDPR imposes.

- You must map where tags are firing from, and control how and when they fire based on user consent.
One tool that can provide an audit of all of the third party vendors on your site is **Evidon Trackermap®**. With this tool, you can conduct live scans of your website and reveal the entire digital ecosystem, including the full redirect chains of third-party vendors, and identify non-secure tags.

As you can see from the example above of the NFL’s (National Football League) site, there can be dozens of tags firing on your site at any one time. You can visit Evidon.com/solutions/trackermap and input your own company’s URL to get a free scan, and an idea of how many tags reside on your website.

### 2. Conduct a site-wide profiling analysis

- Analyze the different visitor profiling activities (tracking) being conducted on your sites. What data are you, your vendors, and their partners collecting, and why?

- Evaluate the various levels of data sensitivity involved in each of these collection activities, and rank the associated risks.

- Analyze what submissions are saved to your site database.
3. Determine the legal basis for data collection activities

Under the GDPR, personal data—including IP addresses, device identifiers and anything else that can be used to identify an individual—can only be collected if you have a “legal basis” to do so.

Examples include:

- it’s necessary to fulfill a contract
- to protect the rights or safety of another
- there is a valid court order
- you have a legitimate interest to collect someone’s personal data, for example, so you can ship a book that she just purchased to her home address.

Absent any a valid legal basis to collect someone’s personal data, then you need to get their consent.

Once you’ve assessed each data collection activity happening on your website, you need to begin to create a process for obtaining permission from anyone that falls into the “Consent” bucket. As mentioned before, consent must be specific to the actual data being collected, affirmative and unambiguous. In the world of digital advertising, where data is collected and exchanged in nanoseconds, this will prove especially vexing.

4. Set up a privacy rights infrastructure

Under the GDPR, consumers enjoy a variety of new privacy rights regarding their personal data, and companies have the obligation to establish internal processes to accommodate this variety of rights. Your enterprise needs to create a channel for visitors or customers to submit any rights requests, and an attendant process for fulfilling them.

Some of the personal data rights under the GDPR:

- **Right to Data Portability:** Your “data subject” (visitor or customer) can receive any personal data he or she has provided to the “controller” (your organization), which that individual can then pass along to another enterprise without “hindrance” from you.
Right to Erasure/Right to be Forgotten: The “data subject” can request that you erase any personal data about him/her, “without undue delay.”

Right to Object: The visitor/consumer can object to you processing their personal data, unless you can demonstrate good reasons for doing so that override the person’s interests.

Right of Access: Individuals have the right to get confirmation from you as to whether or not you’re using their personal data, in which case, they are granted the right to access it.

Right to Rectification: A person can ask you to rectify/correct any inaccurate personal data you’re holding about him or her.

Right to Object to Profiling (by automated processes): This is akin to tracking, and a consumer has the codified right to object to this activity.

5. Design sites around “GDPR consent”

The GDPR specifies a website operator needs to honor “data protection by design and by default.” To ensure you’re meeting the high threshold for valid consent, any user’s on-site experience should allow them to clearly assent by “a statement or a clear affirmative action.”

What are the “design and default” measures to take to ensure that your website is compliant with GDPR mandates?

- A persistent banner must be displayed on the site, requesting users to consent where appropriate. However, they must still be able to access the site even if they haven’t yet given their consent.

- The banner and all supporting information must be in easy-to-understand language, not legalese, and should clearly explain how and why you want to collect their data.

- Silence, pre-ticked boxes or inactivity does not constitute valid consent, nor can consent be inferred through a website visitor’s actions such as going to another page on the site.
Consent is not considered freely given if there's a “clear imbalance” between the visitor and the website operator/company/organization. One weighty example? You can't make a service conditional upon consent, unless the user’s data is necessary for the service.

A user should be able to view a clean and comprehensible list of all vendors and the data being collected, and allow for consent to be specifically given for each.

The user should be told that they're able to easily revoke their consent at any time, and request that their personal data be erased.

The Silver Lining?

Consumers widely fear that companies can't be trusted with their personal data. No less than 71% of them believe that brands with access to it are using it in unethical ways.  

So in some ways, it's like the GDPR serves a second purpose: to save corporations from themselves. How so? Given back control of their personal data, customers have rewarded brands. One example:

- After Facebook implemented (and promoted) a transparent approach to privacy where users could adjust their personal data settings, 61% of users made changes.

- During the same period, Facebook added 467 million new users, hitting a total of 1.86 billion at the end of 2016.

Organizations that embrace GDPR – and publicize the fact they are leading the way towards GDPR compliance – stand to reap the same rewards.

The balance of power in the marketplace is shifting into the hands of the individual. By pursuing GDPR compliance, companies have a unique opportunity for building deeper bonds of trust with their customers and audiences.
TOOLS FOR ACHIEVING GDPR TRANSPARENCY AND CONSENT

Our GDPR Compliance Solution and Trackermap® are easy-to-use, best-in-class solutions for meeting the GDPR consent requirements.

**Trackermap**

The first step to compliance is visibility into the vendors on your company sites and apps.

**Trackermap** provides a 360° view of all your digital technologies including ones you aren't even aware of. The other benefit of Trackermap is that during your analysis, you're likely to find tags that are slowing your site down or not firing properly, helping you to speed up, clean up, and lock down your site.

Use Evidon Trackermap to:

- Reveal your site's digital supply chain of third-party vendors
- Catch potential compliance and security risks
- Optimize site performance by auditing for slow or redundant tags
GDPR Compliance Solution

Developed in collaboration with data protection experts, privacy leaders, policymakers, technologists and marketers, our GDPR Compliance Solution is based upon our existing patented technology – and is the first unified solution to help organizations achieve compliance with the GDPR and other privacy laws requiring notice and consent. Some of its capabilities include:

- Marries ePrivacy and GDPR consent requirements into a single user experience.
- Is built with privacy by design and privacy by default to the highest standards.
- Deploys a persistent notice banner that disappears only once the user has consented.
- Displays granular and specific data collection vendors, and empowers the user with the ability to consent to each, all or none, as well as the ability to withdraw her consent at any time.
- Allows only essential and necessary technologies to fire before consent is given, and then remaining technologies can execute.
- Provides the user a gateway to exercise their GDPR-based privacy rights.


Recently acquired by Crownpeak, Evidon is a global technology company focused on simplifying the complex world of Digital Governance. As companies add more marketing and advertising technology to maximize the return on their digital investment, building consumer trust has become ever more important.

Fulfilling this promise requires organizations to have a comprehensive approach to govern data collection across their sites, apps, and ads while staying in compliance with global regulations.

The world’s leading brands rely on Evidon to empower their Digital Governance success across millions of web pages and apps that drive billions in online revenue.