SECOND EDITION

How to make your website compliant with the GDPR

A 5-step process to help manage the transparency and consent requirements of EU privacy legislation

Contents

Introduction to the second edition 3

What is the General Data Protection Regulation and does it apply to me? 4

What does the GDPR require? 5

What is the risk of non-compliance and is the GDPR being enforced? 6

Turning obligation into opportunity 8

A GDPR roadmap: Five steps to website compliance 9

Tools for achieving GDPR transparency and consent 14

Introduction to the second edition

May 2020 marks the two-year anniversary since the European General Data Protection Regulation (GDPR) came into effect. So how successful have businesses been in adapting their processes to achieve compliance? How has the regulatory landscape evolved? And, what work is still to be done?

It's clear that most businesses are still very much in the foothills of their data privacy journeys. In the rush to meet the compliance deadline, many engaged in a form of "privacy theatre" – meeting the requirements just enough to comply with the new law and avoid fines.

However, this minimal compliance mentality has not gone unnoticed and after an initial grace period, the regulators are set to raise the bar. In June 2019, the UK Information Commissioner's Office (ICO) issued the first in a series of update reports to help advertisers and publishers better understand and address their responsibilities and warned that they'll be checking for progress.

The GDPR's anniversary was also marked by a proliferation of landmark fines as the regulators flexed their muscles. We are seeing serious enforcement, with headline cases such as the $228 million fine for British Airways, the $124 million fine for Marriott, and even the rumored $5 billion fine for Facebook. Smaller companies have been caught in the regulatory crosshairs too, incurring significant costs and reputational damage.

In the wake of high-profile data breach scandals, public awareness of the GDPR and data privacy rights has never been higher, and consumers are expecting much more of brands. Organizations must learn that the price of ignoring regulatory responsibilities goes beyond fines; it also covers consumer trust and experience.

The good news is that for those companies who take their obligations seriously there is much to play for. The ability to deliver secure, trust-worthy customer experiences provides a competitive advantage, and a unique opportunity to set new, mutually beneficial rules of engagement.

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. It has become the de facto global standard informing a raft of copycat legislation from Brazil to Indonesia to Hong Kong. In 2019, 13 states enacted privacy laws or proposed bills modeled after the GDPR, including the California Consumer Protection Act (CCPA) and New York Privacy Act.

Because of its low triggering mechanism, it applies 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, which was inserted into the legislation at the final hour, 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 went 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 it is a central theme of the law.

What does the GDPR require?

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 they 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 assuredly be the case for most website data collection – then the company has to obtain valid consent directly from the individual. To make matters more complex, consent has become 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 rocking the digital advertising industry like nothing seen before, and there is a genuine question around whether it is possible for the adtech industry, as it currently operates, to comply with all aspects of the GDPR. The UK Information Commissioner's Office (ICO) fired a shot across the bows of the adtech industry in 2019 with the release of an Update report into adtech and real time bidding, highlighting their concerns and clarifying expectations. This was followed soon after by the release of additional guidance for publishers on the use of cookies under the GDPR.

While acknowledging the challenges the regulation poses to both advertisers and publishers, the ICO has warned that they consider existing guidance to be comprehensive and applicable and that they "expect to see change."

What is the risk of non-compliance and is the GDPR being enforced?

The GDPR has real teeth to it. Since its inception, more than 200,000 data breaches have been reported, and fines have been imposed in every instance. 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.

As anticipated, data protection authorities have taken robust enforcement actions against the industry giants, providing a cautionary tale for others.

Notable actions include:

- **Google:** In January 2019, the French Data Protection Authority (CNIL), imposed a penalty of €50 million against Google for lack of transparency, inadequate information, and lack of valid consent regarding the personalization of its ads.
- **British Airways:** In July 2019, the UK's ICO announced that it planned to fine the airline £183 million ($228 million) over a data breach which compromised the credit card information of up to 429,000 of its customers. The fine amounts to 1.5% of British Airways' £11.6bn worldwide turnover last year.
- **Marriott:** Also in July 2019, the ICO hit hotel group, Marriott, with a fine of just over £99m ($124 million), for a data breach that lasted over four years, and exposed the personal data of 339 million guests. The fine equates to nearly 3% of the company's global revenue.

While the headlines may have been grabbed by the biggest players, the regulators have also been active in holding smaller organizations to account:

- **Bisnode:** Swedish data-analytics firm Bisnode was fined by the Polish Data Protection Authority (UODO) €220,000 for failure to meet the data subject rights requirements under the GDPR. The fine is small compared to the company's annual revenues of SEK 3.696 million (€343M), but along with the fine, UODO imposed a requirement for the company to reach out to their nearly 6 million users informing them of their rights under GDPR. Bisnode estimates that this will cost them nearly €8M in postage and handling, not including the administrative costs.
- **Vectuary:** In October 2019, French adtech company Vectuary received notice from CNIL to fix their consent solution or cease operations. CNIL has recently withdrawn their notice to the firm after being convinced that Vectuary has addressed its concerns, but it serves as a reminder that a company's revenues don't have to be in the billions to be subject to enforcement.

- **Knuddels:** German social media site Knuddels was hit with a €20,000 fine after disclosing a breach affecting 330,000 of its users. Like the Bisnode decision, the fine doesn't account for any administrative, operational, or opportunity costs incurred by having to deal with the violation.

The fines may not have lived up to the threatened maximum of 4%, but they have been substantial and sweeping. With rising penalties, legal experts are warning companies to check their liabilities with respect to their third-party data processors. Prior to the GDPR, the maximum fine for any data protection violation was £500,000, which has meant that even after the regulation came into effect many contracts continue to reference that figure as a liability cap. Data controllers must now look to negotiate caps that cover them in the event of a maximum GDPR fine, and closely vet the security and compliance practices of the companies they do business with.

In addition to the regulatory penalties, companies must also consider the impacts of remediation costs, reputational damage, and disruption to business. IBM's 2019 Cost of a Data Breach Report estimates that costs have risen 12% over the past five years with midsized businesses particularly at risk of being overwhelmed by the impacts. **The message is clear, regardless of the size of your organization, you need to take action**.

Turning obligation into opportunity

A year after the GDPR came into effect, nearly a fifth of consumers believe their experience with brands has actually worsened, and 40% believe that companies don't take their regulatory responsibilities seriously. In the face of an increasingly savvy and demanding market, firms that aim for the lowest bar of GDPR compliance are missing the opportunity of turning consent and privacy into a way to build relationships with their customers, earn trust, and gain a significant competitive advantage.

The GDPR has shifted the balance of power into the hands of the individual. Marketers know that content is what hooks the attention of consumers and keeps them coming back. But that content needs to be tailored or personalized so they can deliver the right messages to the right audiences at the right time, and this requires access to user data. If businesses want data access, they must reduce friction, and view consent as the first touchpoint of the consumer journey – an opportunity to set new, mutually beneficial rules of engagement. Forward-thinking companies are embracing GDPR compliance as a rich opportunity for building deeper bonds of trust with their customers and audiences.

In the following section, we present **a step-by-step process for achieving compliance with the GDPR consent requirements**. Plus, we 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 five key steps to achieving compliance with the GDPR transparency and consent requirements:

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.

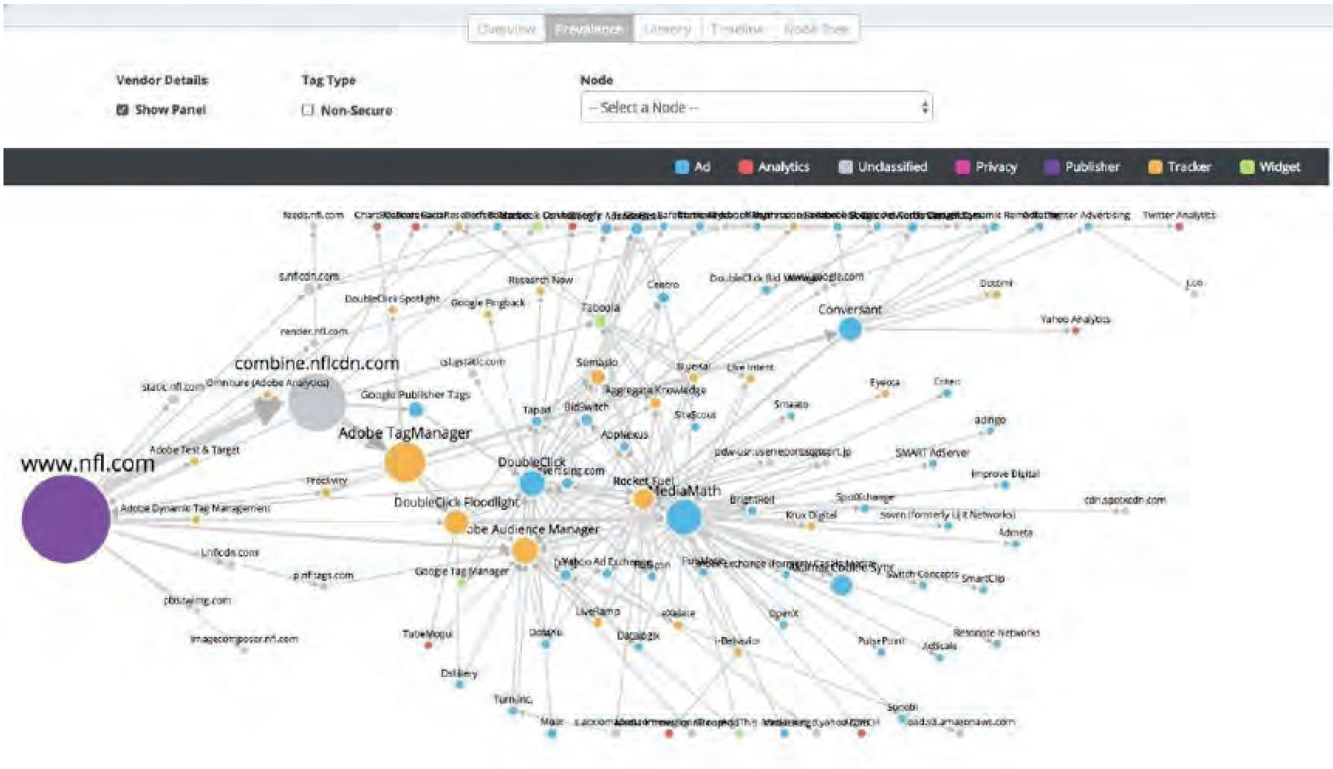
Often, these tags may give data access to other outside firms that the website operator isn't aware of. By permitting those tags on its site, a company is implicitly giving those vendors the right to collect visitor data.

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

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 Crownpeak 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 crownpeak.com/trackermap and input your own company's URL to get a free scan, and an idea of how many tags reside on your website.

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.

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?

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.

Personal data Examples mean 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.

In the absence of 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 is proving 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 grant- ed 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.

Your consent solution is not only the first visible sign to your visitors of your organization's approach to privacy, but it forms the building blocks of customer trust and equity.

By prioritizing transparency and consumer control from the offset, companies can boost the odds of gaining consent, and redefine the customer relationship.

Tools for achieving GDPR transparency and consent

Complying with the GDPR transparency consent requirement is an opportunity for brands to build more enduring relationships with customers and gain a competitive advantage.

Crownpeak's GDPR compliance solutions and Trackermap® provide you with an end-to-end suite of tools to create premium consent experiences that match your brand and tone of voice, promoting trust and user engagement. We call this approach Privacy UX – the privacy user experience as part of customer experience.

GDPR compliance solution

The Crownpeak Universal Consent Platform provides an easy to implement, fast, turn-key solution for even the most complex of multi-site, multi-brand environments. Consent is fully integrated and customizable to your design and user experience choices creating a high degree of trust and visibility for the visitor. Built around flexibility, you decide how best to implement the tool based on your organization's specific GDPR compliance interpretations.

Trackermap

One of the biggest challenges in achieving compliance with the GDPR consent requirements is providing full disclosure of all of the third-party tags and cookies that may be operating on your site. Crownpeak Trackermap gives you a 360° view of all of the third-parties with access to your website and application user data – including vendors you might not even know about due to the hidden, "piggybacked" tags contained within the tags of your official vendors.

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 Crownpeak 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

Boasting the world's largest vendor database, the platform scans your websites and matches the technology on your site to third-party vendors, offering an in-depth view into how a user's data is shared and collected. This unparalleled insight grants your visitors full transparency, satisfying key elements of the GDPR and other data privacy laws around disclosure. Crownpeak's Universal Consent platform is the only consent solution on the market that provides real-time scanning, ensuring your site notice accurately reflects any technology changes on your site and eliminating the risk of compliance gaps.

How our solution compares

Feature/Benefit	Crownpeak Universal Consent Platform	Other Consent Management Platforms
Automated list of all third-party profiling on your website, providing transparency to website visitors	Yes	Limited. Only detects and manages cookie-based technologies
Real-time scanning for all technologies on your site, based on real user sessions	Yes	No
User consent preferences that are managed and stored, ensuring all JavaScript tags don't fire without consent	Yes	Limited. Only detects and manages cookie-based technologies
6,000+ vendor database provides insights into every vendor's data collection and data handling practices	Yes	No
Customizable banners that can be changed to match brand look and feel	Yes	Limited
APIs for enhanced customization, providing full control over how the experience is designed and delivered	Yes	No
Track consent in web, mobile, email, forms, IOT devices, chatbots, and more	Yes	No
Dedicated customer success manager for every account	Yes	No
Consent rate optimization tools and dashboard to help you increase your consent rates over time	Yes	No

Complying with the GDPR can feel overwhelming but is critical to being compliant and earning consumer trust. There are three key elements for you to consider:

- **Get consent compliant as fast as possible:** Crownpeak can help you go live with compliant consent in as few as 7 days.
- **Receive complete auditing and transparency on data sharing.** With the best and deepest database available, Crownpeak will help you properly audit the flow of data to ensure GDPR compliance.
- **Take advantage of the help you need to navigate the technology:** Crownpeak provides named customer success reps for every customer to make sure you have all the help you need to implement and stay compliant.

Interested to learn how Crownpeak can help you secure compliance with the GDPR and other international privacy regulations?

Request a demo today!

About Crownpeak

Crownpeak, the only true cloud-native digital experience platform, offers a suite of powerful tools that deliver the industry's fastest time-to-market across web content management, optimization, governance, accessibility, and privacy UX. Crownpeak helps brands quickly create and deliver digital experiences that build trust and maximize customer lifetime value. On top of its powerful CMS, Crownpeak includes built-in personalization and testing tools, on-site tag and performance monitoring, content governance, and web accessibility. As the leader in customizable privacy experiences compliant with global privacy regulations – such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) – Crownpeak provides the world's only API-based consent-as-a-service system, able to optimize progressive consent across all devices and channels. Hundreds of Global 2000 customers – including Toyota, Healthgrades, and Unilever – rely on Crownpeak to deliver privacy-first and high-quality digital experiences with a quicker time to market. For more information, please go to crownpeak.com.