

GDPR and its Impact on Brand Protection: Everything you need to know



Table of Contents

Understanding the new regulation	4
How will GDPR make brand protection more difficult?	5
How can brands stay protected post-GDPR?	6
GDPR FAQs	7



Understanding the new regulation

Since coming into effect on May 25th 2018, the General Data Protection Regulation (GDPR) has forced many businesses across a swathe of different industries to change how they gather, process, and share personal information. At its essence, the regulation is in place to ensure companies are handling and using their customers' data correctly and responsibly, and so many have had to re-evaluate operations and processes to ensure that they are working in line with the new rules.

Despite the best intentions of those behind the GDPR, its enforcement has triggered a number of unfortunate (and seemingly unforeseen) effects, particularly in the brand protection field. While consumers are more secure thanks to increased data transparency, the GDPR has actually made it more difficult than ever for businesses to stay protected against a number of cyber threats.

Specifically, the GDPR has made it more challenging for organisations to prevent and mitigate the risks associated with counterfeiting, consumer fraud and other forms of online abuse. GDPR has hindered efforts to fight cyber attacks, the physical distribution of illegal pharmaceuticals and threats against intellectual property rights.

Even now that the GDPR is officially in force, businesses are still trying to wrap their heads around the issue and gain a more accurate insight as to how their brand protection efforts will be impacted by the regulation.

This brochure is designed to help brands navigate this tricky terrain by explaining everything there is to know about GDPR and its impact on brand protection. It will discuss how brand protection is negatively impacted by the GDPR and what brands can do to remain safe in a post-GDPR environment. It will then provide answers to some frequently asked GDPR-related questions, as well as a useful further reading/viewing material section for those after some additional knowledge and insight.

The GDPR has made it more difficult than ever for businesses to enforce effective brand protection.



How will GDPR make brand protection more difficult?

The GDPR was not created with the intention to negatively impact brand protection. However, its enforcement has resulted in several indirect consequences that present considerable obstacles in achieving effective brand protection.

The most significant of these consequences are severe restrictions that have now been placed on the WHOIS database. Up until the enforcement of the GDPR, WHOIS played a huge role in all kinds of consumer protection efforts; not just for intellectual property-related issues like counterfeiting and piracy, but in combatting all forms of abuse that takes place on the internet.

With the GDPR now in effect, the WHOIS database is but a shadow of its former self, with far less information available to help brands in their protection efforts. The reason for this is simple: WHOIS in its previous form was not compliant with the GDPR, as it contained large amounts of personally identifiable data (PII), including full names, email addresses, home addresses and more.

In the build-up to May 25th, there was uncertainty as to what might happen to WHOIS. There was a period of time in which many believed – with no alternative option and no sign of WHOIS being given permission under exceptional circumstances to operate in its initial form – that the database would be forced to shut down entirely. This would have been catastrophic for brand protection efforts.

Thankfully, just days before enforcement, the Internet Corporation for Assigned Names and Numbers (ICANN) implemented a **Temporary Specification** that would allow WHOIS to remain operational, albeit in a severely limited form. This new model shields all available registrant-related PII from public access, save for the organisation name, state/province and country, as well as an anonymised email

“With the GDPR now in effect, the WHOIS database is but a shadow of its former self.



address that is the only method of communication for the registrant. While not as catastrophic as a total blackout, this model does make it far more difficult to monitor and manage brand protection threats with the same level of detail and attention.

This seems to be one of several entirely unintended consequences of the GDPR coming into force. If experts could have predicted this would happen in the first place, European authorities would surely have made every possible effort to keep WHOIS up and running in its original form. It is counterintuitive to overvalue privacy to the point where it jeopardises the public interest which is protecting those same citizens.

How can brands stay protected post-GDPR?

While the unfortunate fate of WHOIS has no doubt made effective brand protection more difficult, there is hope for brands on the horizon, and still things that can be done to stay protected in the meantime.

Most importantly, ICANN is hard at work developing an official accreditation and access model which would effectively give authorised parties (i.e. brand protection companies such as *MarkScout*) access to the information on WHOIS that is shielded from public access. This would ensure all WHOIS data is available to those that need it the most, but there is still some work to go before an accreditation and access model is created and approved by all relevant parties.

Of course, another option is to stop relying on WHOIS altogether and find an alternative source of information to aid with brand protection. MarkScout has its own alternative solution – an extension of our brand protection capabilities that enables businesses to maintain effective brand protection efforts through the automated provisioning of data from third-party sources.

 **MarkScout's**
*technological solution
enables businesses
to maintain effective
brand protection
efforts through
the automated
provisioning of data
from third-party
sources.*

Whether equipped with a technological solution or not, this post-GDPR era will definitely involve more manual work in order to continue dealing with brand protection threats. Certain cases might involve sifting through different websites and pages to gain the information that's needed to shut down a domain – and this might well require additional resources.

Finally, when all else fails, the court can get involved. Obtaining a subpoena or court order might be the only way to access the registrar or registrant information needed to make the necessary enforcements. If this avenue is chosen, brands should take into account the fact that the costs of litigation will no doubt increase.

GDPR FAQs

All brand protection experts have their own set of questions when it comes to the contentious issue of GDPR. For those wondering about the finer details of the regulation or about the impact to WHOIS, we have compiled some of those most frequently asked questions.

Why are registrars deciding to hide registrant data?

ICANN approved a **Temporary Specification** for the display of WHOIS data in late May, just days before the enforcement of GDPR. Registries and registrars are required to follow this specification, which allows them to mask all registrant data, regardless of whether the registrant is a resident of the European Economic Area or not.

Apparently, some registries and registrars have decided to display some registrant data. Is that allowed?

Some registries and registrars – in particular those who sell and provision country code top-level domains (ccTLDs) – are not subject to ICANN's contracts or policies. Some have also found that certain information within WHOIS, such as registrant email addresses, can be published without violating the GDPR, according to local law. Because circumstances differ from case to case, it is recommended that registrars follow the advice of their own legal counsel on this matter.

How will the changes to WHOIS impact MarkScout's ability to enforce IP rights?

With no access to registrant information on WHOIS, our ability to perform reverse domain name lookups and anonymous domain name acquisitions will undoubtedly be hindered. It will still be possible to do website enforcements, but they will require more effort on the part of analysts to find reliable registrant contact data on infringing websites. All other services will remain unaffected.

What efforts are underway to mitigate the impact of WHOIS on MarkScout enforcement efforts?

After assessing the impact of GDPR on our services, we've devised three unique solutions. Firstly, we are hiring additional brand analysts to assist with the manual effort required to

“It is still possible to do website enforcements post-GDPR, but they will require more effort on the part of analysts to find reliable registrant contact data on infringing websites.

search websites for registrant data. Secondly, **we’ve deployed world-leading technology** capable of tracking down data to determine the identity of a registrant. And finally, we’re proactively engaging with third parties to stay on top of our efforts to identify IP infringement.

How long will WHOIS remain in this redacted form?

No one knows, but at least for several months. Progress has been delayed due to the struggle in getting an accreditation and access model approved. Once approved, this will be a significant step forward in opening up WHOIS to those that need it the most.

MarkScout is also actively participating in advocacy efforts at ICANN, with other corporations, associations and non-profit organisations, to design, develop and implement an access model as soon as possible. It is also worth keeping in mind that an approved model will take around nine to twelve months to implement.



About MarkScout

MarkScout provides online brand protection and domain management for global brands. Our technology and experts detect and remove counterfeits, piracy, fraud and brand abuse across marketplaces, social media, domains and the dark web, helping protect revenue, reputation and customer trust. To learn more, visit markscout.com.



LEARN MORE

[MARKSCOUT.COM/ SERVICES/BRAND-PROTECTION](https://markscout.com/services/brand-protection)