

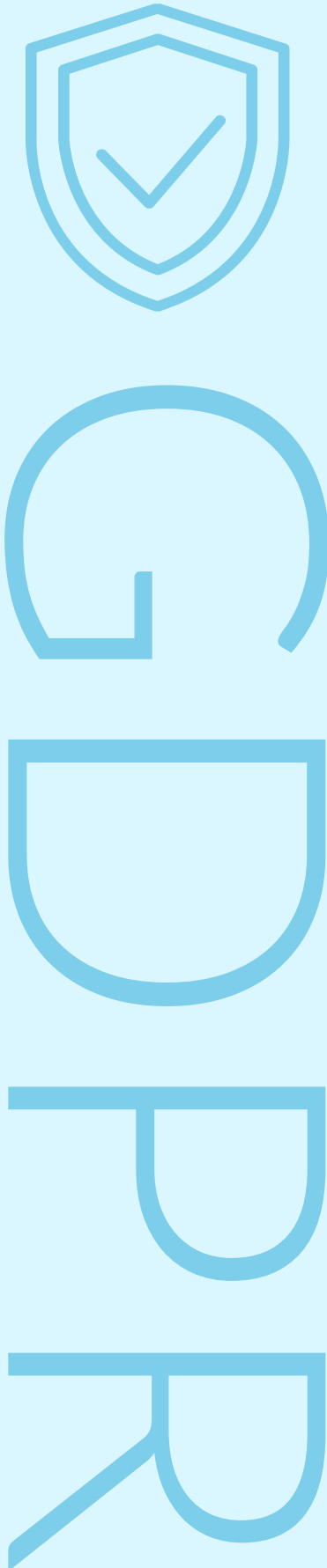


General Data Protection Regulation

The new
landscape
for enforcing
and acquiring
domains.

You've built your business and
your brand. Now how do you
secure and protect it?





CONTENTS

- [01](#) Introduction
- [01](#) Overview
- [02](#) WHOIS Under GDPR
- [03](#) New Era
- [03](#) Private Registration
- [04](#) WHOIS Stakeholders
- [04](#) Domain Investors
- [05](#) Trademark Owner
- [06](#) Intellectual Property
- [07](#) Gated WHOIS
- [07](#) Cybersecurity
- [08](#) Enforcing & Acquiring Domains



INTRODUCTION

The European Union's newest addition to the Data Protection Directive, the General Data Protection Regulation (GDPR), coming into effect on May 25 2018, has altered the business world's obligations in handling personal data and privacy practices surrounding this data. As a consequence, the structure of a critical piece of the domain name system, the WHOIS database, has been questioned to its core.

ICANN's Temporary Specification, meant to address these questions around WHOIS, is only in effect until May 25th, 2019, while ICANN and its contracted parties are working on a permanent policy that addresses the internet community's concerns around WHOIS while remaining compliant with GDPR.

In the meantime, companies will need to adapt to a domain system deprived of public WHOIS information and understand how it will impact their ability to enforce and acquire domains.

OVERVIEW

WHOIS has always been at the center of a long-running debate with many parties challenging the ability of WHOIS to meet the needs of today's savvy Internet users. The WHOIS database was established to collect and display information about domain name registration records from registries and registrars in real-time.

As the Internet grew, contact information listed in WHOIS began to serve the needs of new stakeholders including domain name investors, intellectual property owners, law enforcement agents, businesses, and individuals.

With the evolution of the Internet, the public domain record information began to be used in ways unforeseen by its creators. As well as being an aid for legitimate parties, WHOIS has also become a resource for fraud and abuse.

Although the WHOIS system has been modified over the years, its future has never been put into question like it is today with the GDPR.

WHOIS UNDER GDPR

Domain registrars are doing what they can to create ad hoc solutions that satisfy WHOIS requirements and still comply with the EU's GDPR. Many domain registrars redacted personally identifiable information of domain registrants from their WHOIS database in compliance with ICANN's Temporary Specification for gTLD Registration Data, a short-term solution created to satisfy GDPR regulations.

A few of the larger registrars dedicated staff resources into developing a new technology that can display WHOIS information geographically in a way which excludes European Union citizens. Many registrars have not been able to implement a new system as quickly. Instead, they have opted for an easier solution which shields everyone's WHOIS information by default regardless of where they reside.



Registrars are required by ICANN to adopt a system that allows for an open door of information. Today, with the introduction of the GDPR, the door of free-flowing information is closed and only under predefined circumstances can the door be opened and information released. Registrars are utilizing new systems to comply with ICANN's Temporary Specification. Registrars must redact any personally identifiable information of the domain registrant and publish only pertinent and non-sensitive information.

In addition, they must also offer a web form to contact the domain registrant or provide anonymized emails for domain owners in the WHOIS record. Cira is a domain registry that has been successfully utilizing this system for years in management of .CA Canadian domains. Since its launch in 2010 Cira's Interested Party Contact: Message Delivery Form is proud to facilitate over 250 secure messages a month while keeping the domain owner's identity private for over 2.7 million domains in operation.

NEW ERA

Even with ICANN's Temporary Specification restricting domain operators from publishing registrant data to the WHOIS database, Private Registration remains a valuable tool.

There is a continued need for privacy services to protect domain registrants. As a company policy, 101domain redacts all of our customers' personally identifiable WHOIS information such as name, phone number, and email address, not only those that reside in the EU. However, we are still required to share the information of each domain registration with many of the registry companies that operate the domains.

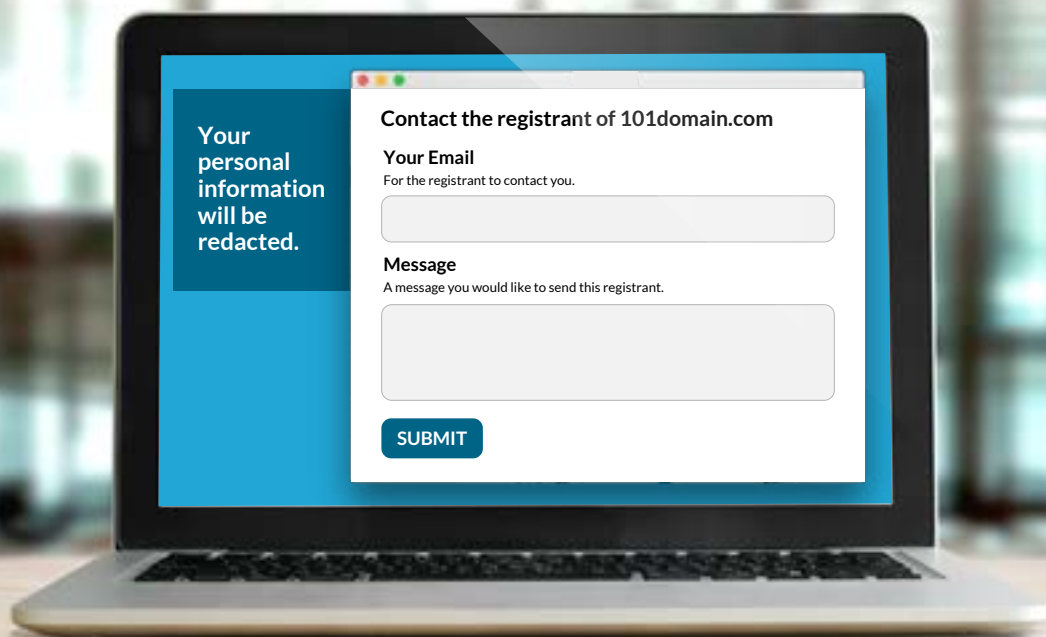
Many registrars and registries are responding to the GDPR by masking WHOIS information, but others, such as several country code domains, are not necessarily held subject to GDPR regulations and continue to publish these records. Some domain companies continue to display domain registrant information on their WHOIS output, leaving domains without Private Registration susceptible to having their personally identifiable information available as a public record.

PRIVATE REGISTRATION

In order to comply with the GDPR and ICANN's Temporary Specification, we redact all of our domain registrants personal information from our public WHOIS output. However, in order to complete the registration, we are required to send the domain registrant information to many registries including those that fall outside of the GDPR jurisdiction and therefore are not held accountable to EU law.

Some country code domain registries publish WHOIS information for the purpose of public research. This information may be scraped and used in solicitation campaigns.

101domain will continue to offer Private Registration services to further protect our customer's privacy. Adding Private Registration ensures a domain registrant's records will be replaced with the contact information of our privacy service and their personally identifiable information masked from all parties except when required by legal or contractual obligation. This way, all legitimate requests are received with none of the spam.



WHOIS STAKEHOLDERS

There are many stakeholders intent on preserving WHOIS even if in a limited form.

Domain investors rely on a public WHOIS to help conduct their business of selling domain names.

Intellectual property owners research domain registrant WHOIS information to protect their online assets and identify the correct party to serve copyright takedown notices, trademark infringement cease and desist demands, and complaints under ICANN's UDRP or URS policies.

Law enforcement agents and cybersecurity professionals use WHOIS information to identify trends and reduce criminal activity online.

Domain registrants seeking a higher level of online privacy have always been able to achieve this through Private Registration services, but with the introduction of the GDPR and ICANN's Temporary Specification, limited WHOIS information has become the new protocol.

DOMAIN INVESTORS

Without WHOIS information, users cannot easily identify the owner of a domain name, even in the case where they want to be found.

Unlike most people on the web, domain investors want their private information available to the public.

The long-term solution to replace ICANN's Temporary Specification will most likely include an option for customers to opt-in to having their information displayed on WHOIS. This opt-in feature would benefit domain investors by giving their portfolios more visibility.

Without personally identifiable information being publicly displayed, there is more room for assumptions to be made about whether a domain was registered in bad faith.

Let's say Joe Smith registered `jsmith.com`, but a retailer of denim jeans, J. Smith Jeans wants the domain `jsmith.com`

It will be more difficult to identify the intent of a domain owner and if they have legitimate interest in the domain or is commonly known by the domain name.

This is an example of one of the many challenges in a domain industry without a fully transparent WHOIS.



TRADEMARK OWNERS

The Uniform Domain Name Dispute Policy was put in place to help trademark owners recover domain names that were registered in bad faith. In cases of trademark infringement, a brand owner can file a UDRP or URS complaint with an ICANN accredited entity in order to have the domains suspended or transferred to them if the brand owner prevails. With the new implications of the GDPR this has become complicated.

IP professionals traditionally use WHOIS information to aid them in recovering and acquiring domain names for their clients. Without public WHOIS information, complainants filing UDRP and URS cases are essentially going into them blindly. This can be extremely frustrating for trademark owners who are trying to prove infringement of their brand. Without being able to easily identify the domain registrant it is difficult to determine the intent of the user, whether they are an established domain investor, an honest business person, or a cybersquatter who registered the domain name in bad faith.



51.3% of all UDRP complaints are filed from trademark holders located in the EU, with 23.1% of all domain owner respondents also residing in the EU.

wipo.int/amc/en/domains/statistics/

The World Intellectual Property Organization (WIPO) described how this will work under the GDPR. In a two-step process, the complainant will file a case, at which time WIPO will recover the domain owner's information from the registrar.

At this point, the complainant can decide to continue or amend its complaint based on the personally identifiable information they now have. This process takes additional steps which creates a more extensive process.

The previous system which had access to WHOIS, allowed trademark holders to conduct research on their own and determine if there was a case of trademark infringement before they took action under the UDRP.

Without being able to cite multiple domains under the same domain holder, the average domain names per complaint will decrease in this new process as will the effectiveness in recovering cybersquatted domain names.

WIPO Two-Step Process For Filing a Complaint

STEP 1

Trademark holder files a complaint with WIPO

WIPO turns over domain owner's information

STEP 2

Trademark holder decides whether or not to pursue the case



INTELLECTUAL PROPERTY

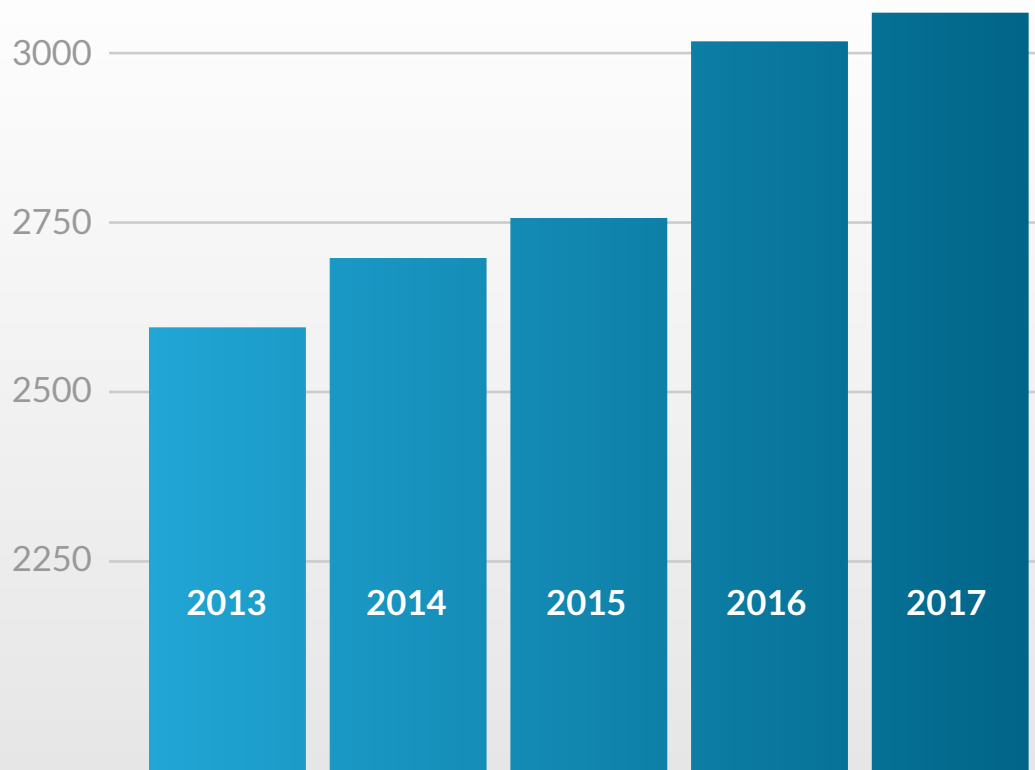
Moving forward, domain investors should use parked pages to reflect the proper use and intent of their domains and when available in future ICANN policy, opt-in to their WHOIS information being shared publicly with their domain registrar.

Businesses and individual users would benefit from utilizing Private Registration services to further protect their information, while trademark owners and intellectual property professionals will need to work harder when it comes to acquiring and enforcing domain names in this new space.

WIPO Domain Name Disputes

■ Number of cases

wipo.int/amc/en/domains/statistics/cases.jsp
January 2018



GATED WHOIS

Law enforcement and the GDPR share a common interest in protecting the security of individuals. However, even with this shared resolution, the current GDPR regulation restricts the availability of WHOIS information to law enforcement agencies.

The future ICANN specification will include a gated WHOIS that will allow law enforcement and cybersecurity professionals access to WHOIS data. Some concerns delaying the approval of a gated system revolve around regulation of the data and ensuring it will be used for its intended purpose. A gated system will need to balance the interest of law enforcement and the privacy of EU individuals.



Anything that limits or restricts the availability of Whois data to law enforcement agencies will decrease its usefulness in FBI investigations, while anything that increases the accuracy and completeness of Whois data will improve timeliness and efficiency in our cases.

James E. Farnan; Deputy Assistant Director, Cyber Division, Assistant Director, Cyber Division; Federal Bureau of Investigation

CYBERSECURITY

There is a misconception that WHOIS information does not help law enforcement and cybersecurity personnel from identifying perpetrators.

Some argue that criminals registering domain names for illegal activity wouldn't be careless enough to use accurate information, therefore making WHOIS data of no use to these investigative parties.

In reality, any information that can identify patterns in personally identifiable information, even if inaccurate, can help law enforcement agents target criminals and eliminate cybersecurity threats.

Criminals will re-use registration information across many domains and cybercrime campaigns to avoid the hassle of creating new email addresses, phone numbers, addresses etc. The proper authorities can use this public information to determine the parties responsible.



According to KrebsOnSecurity, WHOIS proves useful in mapping the extent of malware and phishing operations even with inaccurate and misleading information.

Until a long-term solution is approved, law enforcement agencies will need to adapt to a system with limited WHOIS access in the greater goal of protecting online users.

ENFORCING & ACQUIRING DOMAINS

Enforcing and acquiring domain names under the GDPR proves to be a great challenge. With limited WHOIS, domain investors need to work harder to be found, while trademark owners and IP professionals require greater investigation in building cases and recovering domain names.

The success of the GDPR within the domain industry will depend on the community's ability to adapt and create solutions that provide value for all parties involved.

A gated WHOIS system appears to be staged to become the standard industry solution for facilitating communication for acquiring domain names, enforcing IP and legal interests, and protecting the privacy of Internet user's personally identifiable information.

In a short time, if anything, the GDPR has been successful in sparking a global conversation around the topic of online privacy and inspiring permanent change in the domain industry.

Time will tell if stakeholders can come together and implement a solution that meets the needs of all parties involved.



www.101domain.com
corporate@101domain.com
877.983.6624

