enom

GDPR Webinar Q & A

We had a great turnout for our GDPR webinar, and attendees asked many intelligent and insightful questions about the regulation and our implementation of its requirements. Since we could not answer all the questions in the two webinar sessions, we wanted to share the responses here for everyone. Below you will find the Q&A; we hope you find it helpful as you work through your own GDPR compliance efforts. If you were unable to attend the webinar in person, we've **posted it on our blog** for you to watch when convenient for you.

General GDPR Questions

Q: Compliance sounds as simple as gaining consent from clients. If their consent has been given, then I'm covered under the GDPR, right?
A: It's not that simple, in part because there are clearly defined limitations around what constitutes legitimate consent, all of which are outlined in our **Consent** blog post. Furthermore, the GDPR's requirements go beyond consent to include things like data minimization, secure processing and storage of data, and more. I can say that from the domain services perspective, we've got things covered. This compliance will be achieved through a combination of contract-based and consent-based data processing and data minimization. If you are collecting and storing personal data for your own purposes, beyond what is required by us, we recommend that you talk to a lawyer who is familiar with the GDPR to fully assess the risk that you're taking by not updating your own processes to comply with the new law.

Q: How will the fines for non-compliance be monitored and collected, and who will be enforcing them against US companies?
A: Each EU country, and in some countries each region, has a Data Protection Authority (DPA) who enforces the GDPR. If you have a presence in an EU country, that is likely the DPA with whom you would interact. If you do not, the DPA of the country where the violation occurred would probably be the enforcer. The enforcement process will rely on reporting, meaning the EU has not indicated that it plans to conduct audits, but instead will investigate potential GDPR violations as they are brought to the DPAs' attention.

Q: Will Nominet terminate the registrant address verification process?
A: This is a question that should be addressed to Nominet, but we are not aware of their having any plans to do so.

Reseller Requirements

Q: What is the allowed time limit for the changes to take place on the side of the reseller?
A: First off, if you collect and process the data of EU-locals, or have the potential to, you need to ensure you are doing so in a GDPR-compliant manner by May 25, 2018. Otherwise, you are putting your business at risk. In addition, our **agreements with resellers will be updated** to require that resellers process data in a GDPR-compliant manner. As for changes that must be made on the reseller's side which specifically relate to Tucows' domain registration processes and modifications to our platforms, there are no mandatory changes you need to make, but there are changes on our end that you need to understand and adjust for if you feel it necessary. One such change is our **new Whois system** (**see "Whois - General" below**). Another is the introduction of the consent management page for end users, the details of which we address in **another response**. On that note, we are not expecting to have consent for all the millions of domains on our platform from day one (May 25), but by requesting consent at the time of domain registration, renewal, or transfer, we expect that the majority of the registrants in our system will have indicated their consent selection within the first year of this requirement being active. You should consult with your lawyer to determine how to handle consent collection and overall GDPR compliance for your own business.

Q: Do you recommend any particular software to help companies prepare?
A: No, but I would recommend consulting a lawyer who is familiar with the GDPR and our industry.

Q: Is the OpenSRS/Enom email system being dealt with separately?
A: Yes, this webinar focused on the wholesale domains platform. Hosted email is being handled separately and presents far fewer challenges. This is because email is a secondary service that doesn't actually require the collection or processing of additional personal data: we simply attach an inbox (or inboxes) to the domain name. At present, we are planning to make minor adjustments to our email service, neither of which will be reseller-impacting.

Q: When will you publish the final updates being made to your contracts?
A: While we appreciate that uncertainty around these changes is difficult, we hope that an industry-standard amendment will make things easier for both our resellers and the industry as a whole. At the same time, we know that we can't wait too long before sharing those changes with you. If the industry-wide amendment is not ready for distribution by the end of March, then in early April, we will release our own contract changes to our partners.

Q: Does everything described today apply to both OpenSRS and ENOM customers?
A: Yes. We're applying the same compliance strategy and process across the board, though the visuals, such as emails, landing pages, etc., may have superficial differences.

Q: What role does Data443 have in your compliance efforts, if any?
A: None; they seem to be doing interesting work, but we are developing our own in-house solutions for data inventory and management.

Consent and Identity

Q: You list the data elements required by contract as: name, organization, email, country. Why are organization and country required to perform the contract?
A: This was determined by our legal team to be the minimum set of data that we require in order to identify an individual such that they can enter into a contract for services with us. Here, context becomes very important. The policy conversation inside ICANN about how to reconcile conventional ICANN requirements for data gathering and Whois publication is ongoing, and some possible implementations may use organizational status and/or country of registrant as pivot points for differing treatment of registrant data. In addition, as privacy-related policies around the world evolve, knowledge of the organizational status and country-of-registrant will allow us to determine the degree of data protection afforded the registrant.

Q: How does the law address proving identity? As an example: I can create a domain using the registrant name "Donald Duck". If another Donald Duck discovers this and asks for the info to be removed, what proof must he provide to verify that he is, in fact, the same Donald Duck that registered the domain?
A: The choice to give consent, and the related ability to request erasure of one's personal data, is all tied to a user profile which consists of a unique combination of the data elements we require contractually: name, organization, email and country. If two registrants share the same name but have a different organization, email, and/or country, they are considered to be two separate people, with distinct user profiles in our system. If a request for erasure comes in from someone who does not match the full contact data set associated with a domain, but that someone still claims to be the registrant and data subject for that domain, our Compliance team would work to address the issue.

Q: When will the API functionality to send the consent request be available?
A: As soon as possible; we are working on this now.

Q: Is there a default consent process of any kind? For example, if the customer does not respond to your consent request within a given window of time, are they automatically considered to have consented or not consented?
A: We will default to a non-consented status after approximately 10 days in cases where we receive no reply from the registrant.

Q: What if the registered domain owner is a Business, not a natural person?
A: We are applying the benefits of the GDPR to all registrants on our platform, regardless of their status as a business or individual. In all cases, the domain would still be applied to a specific user profile, and as such, would need to have a consent status on file.

Q: What happens to pre-existing data, and do we need to send the consent management landing page link to all existing users?
A: Data that is used to perform the domain registration contract will be maintained in our system for as long as is legally required. For pre-existing data that now requires consent, we will request that consent on a timeline that has been deemed appropriate by our Legal team. We will send the consent management landing page link to the end user at three potential points in the domain lifecycle: when new registration is created, when a domain transfers into our system, or when a domain is renewed. Additionally, resellers may send out the link at their discretion via the option that will be in the control panel or the new API call that we will be offering.

Whois - General

Q: Will reseller details still be displayed?
A: The Whois output for domains registered through OpenSRS currently displays the reseller details and will likely continue to do so after May 25, 2018. This information is not currently included in the Whois output for domains registered through Enom, but it is something we are exploring for the future. We're not 100% certain if the reseller info will continue to appear in the Whois record, as it's not mandatory that we provide it there. It's also important to note that we do not plan to disable the reseller lookup functionality available at tucowsdomains.com, which serves a similar purpose.

Q: Are you going to restrict Whois info on our behalf?
A: Yes, we will take care of the Whois output, so resellers can continue to send the same info to us that they do today and rest assured that it will be handled appropriately.

Q: If only the name, country and e-mail address is required, what's to stop me from submitting fake information? For example, I could sign up with example.email@example.com?
A: For legal reasons, such as ownership disputes, it's important that the domain contact information be valid and accurate. Additionally, the Registration Agreement, which all domain owners accept as part of registering a domain through a Tucows partner or reseller, confirms that all information provided will be accurate, current, and reliable. These are contractual requirements, and registrants risk having their domain suspended or canceled if these requirements are not met.

Q: Are you saying name, email, and country will always be displayed and cannot be opted out of (unless we use privacy protection)?
A: If you are referring to those data being displayed in the public Whois, than the answer is no, quite the opposite. By default, those data will not appear in the public Whois. However, they will appear in the gated Whois unless privacy protection is active on the domain.

Q: Are you going to restrict Whois info on our behalf?
A: Yes, we will take care of the Whois output, so resellers can continue to send the same info to us that they do today and rest assured that it will be handled appropriately.

Q: Will there be an option to enable and disable Whois?
A: If this question refers to public Whois, then no, at this time, we are not making it an option to choose to display personal data in the public Whois. The ability to enable or disable Whois Privacy will remain available and continue to work as it does today. You can check out our **Whois changes** post for more information**.**

Q: Can a non-EU domain registrant waive the protections and keep their data public?
A: Not at this time. We believe that providing such an option puts data at risk and exposes it unnecessarily, but this is currently the subject of discussions within ICANN and with various European DPAs, and we will reevaluate our implementation from time to time in light of further policy developments and guidance received from government authorities.

Q: You say "the public Whois has placeholder public data." Will the public Whois output still display domain dates, status, and sponsoring registrar?
A: Yes. The technical data (the top section of current the Whois output) will show up in the public-facing lookup.

Q: Will we be able to see the name servers of domains not in our reseller accounts? Customers frequently ask us to help them move from an existing provider, which requires this information.
A: Yes. The technical data (the top section of the current Whois record), which includes the name servers, will continue to be displayed in the public-facing Whois lookup.

Q: Will we be able to see the Whois data for new customers that we are in the process of transferring into OpenSRS/Enom?
A: If the domain is not yet transferred into your reseller account, then the visibility of Whois data depends on the registrar that the domain is coming from. As we work through the modified transfer process (**see question below**), we can get a more specific answer to this concern.

Q: How can we verify a domain-validated SSL certificate without being able to view the email address
in the Whois?
A: We are currently working with SSL providers to address that concern, and will share our solution with you as soon as we're able.

Q: Why isn't the Registrar's contract with ICANN sufficient for sharing data in public Whois under the GDPR?
A: There are a few reasons for this:

1. The concept of "data minimization" in the GDPR requires that only the minimum data required to fulfill the data subject's request is solicited from data subjects. The data required by ICANN contracts has not been minimized. For example, Admin, Billing, and Tech contacts are required for historical reasons but are not technically necessary in order to register or establish ownership of a domain. So the ICANN requirement does not align with the GDPR.
2. There are contracts between ICANN and the registry, ICANN and the registrar, and between the registry and registrar. According to the GDPR, processing data based on a contract is only valid if the data subject is party to that contract. The domain owner is not actually party to the contract between ICANN and the registrar or registry, so the contract does not cover this data use.
3. The data subject requested the registration of a domain, so any contract with the registrant can only cover data processing required to register that domain or justified by another legal basis (e.g. legitimate interest). Publishing data in a public Whois, for example, is not necessary to register the domain, and the rights of the registrant arguably outweigh the legitimate interest of a public Whois.

Q: How will domain transfers work moving forward? If a reseller cannot see who owns a domain how can they initiate its transfer with confidence that the request is legitimate?
A: As mentioned in the question, the problem with continuing to use the transfer process as it stands today is that the gaining registrar would not reliably know where to send the initial Form of Authorization (FOA), since the registrant email will no longer be publicly available to them. To address this issue, the Registrar and Registry Stakeholder Groups' joint TechOps (Technical Operations) sub-group has sent a **letter to ICANN**, proposing changes to the transfer process. They suggest that the initial Form of Authorization should be optional, and instead, possession of the transfer authorization EPP code will be required to initiate the transfer. Then the current registrar, which does know the owner's email, would send a mandatory confirmation FOA (this FOA is currently optional), and the transfer would only proceed if the domain owner completes the FOA sent by the current registrar within 5 days. The letter in which this change was proposed was sent to ICANN very recently, so we don't yet know how ICANN will respond. Changing the transfer process is not a simple task, as it's a consensus-based policy with a specific protocol that must be followed to approve any modifications. Each registrar will have development work to do once the course of action has been determined, but domain community is united in working towards a timely and viable solution.

Whois - Gated

Q: Will resellers still be able to see all available Whois data or will they we be required to use the gated Whois?
A: Resellers will be able to access all the Whois contact data that we hold for their end-users within the Reseller Control Panel, just as they do today.

Q: In gated Whois view, you're still showing address and phone number data. So you'll still potentially collect those pieces of data on a consent basis?
A: Yes, exactly. Any pieces of data we have consent to process will be displayed in the gated Whois, unless, of course, the domain is privacy-protected.

Q: Will the gated Whois affect non-EU domain registrants?
A: Yes. We are applying all GDPR-related process changes platform-wide, meaning all registrants will receive the same level of data protection regardless of citizenship or location.

Q: Do you have examples of what types of authorities will have access to the "Gated Whois"?
A: We expect that various law enforcement agencies will be accredited for access, and possibly other groups such as intellectual property lawyers and members of the security community.

Q: Would law enforcement need to contact Tucows directly to obtain any "hidden" information, or would they reach out to the reseller?
A: Law enforcement authorities currently contact Tucows to obtain data that is hidden with Whois Privacy, and will continue to do so once the gated Whois system is live. Similarly, in the future, when they need access to the gated Whois, they must request it from Tucows directly because we control entry to that system. That said, they may also contact the reseller.

Q: The current system in place requires law enforcement to have warrants or legal grounds in order for them to obtain the Whois information for a privacy-protected domain. If they get access to the gated Whois, does this mean that they can access this information without having to provide proof of legal grounds to get the data?
A: Access to the gated Whois will only reveal information which is currently (prior to May 25 2018) public. It will not reveal the Whois information for privacy-protected domains. In fact, the Whois output for privacy-protected domains will be the same in both the public and gated Whois, and we will continue to require a court order or other legal documentation for access to this information, as we do today.

Whois - Privacy Service

Q: On the "Do We Still Need Whois Privacy" slide, it said "Data may be legally required in the public Whois" — why would data be legally required in the public Whois?

A: Currently, no legal basis for publishing Whois data has been determined, and thus, the public Whois will effectively "go dark" on May 25th, 2018. However, there's an ongoing industry conversation about what the legal basis for publication could be; as that progresses, a legitimate legal basis may be identified.

Q: In the short term, so that domain Whois data is GDPR compliant, do all customers need to be placed behind a domain privacy service, or should we be making changes to hide data that doesn't need to be made public?

A: Tucows will take care of ensuring our Whois system is GDPR-compliant; no action is required on the reseller's part. For domains that are protected with Whois Privacy, the public Whois output will remain the same once the GDPR is in effect. For domains without Whois Privacy, all personal data will be removed from view in the public Whois but will be accessible via the gated Whois. So no, you do not need to place all your customers behind a domain privacy service. However, we recommend that you continue selling Whois Privacy, as it still presents benefits to the end user. To learn more, please see our **Whois changes blog post**.

Q: What will the difference be between the gated Whois and the domain privacy Whois?

A: The gated Whois is a portal where accredited third-parties can access "full" Whois information, and the output available here will include personal data that will be hidden from the public Whois once the GDPR is in effect. However, the Whois output for domains with Whois Privacy will remain the same as it is now, both in the public Whois and in the gated Whois. This means that Contact Privacy details, including a contact privacy email, will be displayed for domains with Whois Privacy in the gated Whois. For a helpful visual snapshot of the difference, check out our **Whois changes post**.

Q: Can we run our own privacy service, i.e. have our information show in Whois?

A: This is a complex decision for a reseller to make, for a few reasons. There are requirements in our Reseller Agreements around what privacy or proxy services may be used for domains on our platform. Additionally, ICANN has requirements for any privacy or proxy provider and is working now on an accreditation process for providers of those services. We encourage any reseller to review their options with the help of their legal counsel and the operative reseller agreement before beginning to offer such a service.

Q: The sample Whois Privacy Output slide shows a registrant phone number — is that correct?
A: The Whois Privacy output currently shows, and will continue to show, a phone number, but it's a Contact Privacy service number, not the registrant's real phone number.

Q: Will the domain privacy number continue to be displayed?
A: Yes, it will, as this number is not considered personal data. Contact privacy customer numbers are unique to the domain, not the user.

Q: For TLDs that do not support private registration or only support it for certain registrant types (like certain ccTLDS), is it correct to assume that registrant data will be protected via the gated Whois, but registrants will continue not to have the option to add privacy to keep their actual data out of the gated Whois?
A: Yes, that is correct.