Impact of the GDPR on domain registration

Synopsis of the SIDN webinar held on 5 April 2018

Date
5 April 2018

Page
1/7

Contact
T +31 (0)26 352 5500
support@sidn.nl
www.sidn.nl

Offices
Meander 501
6825 MD Arnhem
The Netherlands

Mailing address
PO Box 5022
6802 EA Arnhem
The Netherlands

Michiel Henneke (Marketing Manager at SIDN) welcomed viewers and introduced the contributors: Peter Kager (lawyer at ICTRecht) and Chiel van Spaandonk (Whois Process Owner at SIDN).

Michiel described the agenda of the webinar:

1. Introduction (Michiel)
2. Legal implications of the GDPR (Peter)
3. How the Whois will change (Chiel)
4. Q&A

1 Introduction

- The General Data Protection Regulation (GDPR) comes into effect throughout the EU on 25 May 2018.
- All organisations that handle personal data will be affected.
- Personal data = any information that can be traced back to a natural person. Therefore even information connected to a business registration can be personal data.
- The registration of a domain name involves linking information about the domain name to details of the registrant.

Michiel wound up the introduction with a poll. Webinar viewers were asked: have you aligned your processes with the GDPR yet? Of the respondents, 8% said that they were ready for the GDPR, 74% said that they were working on it but some details still required attention, and 18% said that they hadn't yet begun. Peter confirmed that the results were in line with what he was seeing in practice.

2 Legal implications of the GDPR

Peter introduced himself: he is a specialist in privacy law at the Amsterdam law firm ICTRecht, which represents clients in the ICT industry, including many registrars. He explained that he wasn't going to discuss all the ins and outs of the GDPR, simply how it affects the registration of .nl domain names.

What is privacy? Privacy is about your personal life being safe from unwanted intrusion. Everyone is entitled to privacy, from celebrities to the man and woman in the street. Legally, privacy is a fundamental right, like freedom of expression and freedom from discrimination. For a long time, it was the 'poor relation' amongst fundamental rights. In recent years, however, people have started to take privacy more seriously; the recent furore over Cambridge Analytica being a good example. The GDPR is the EU's response: putting privacy on a firm legal footing.

The GDPR applies throughout the EU and has implications for organisations worldwide. It places obligations on data controllers and data processors based in the EU (those terms are explained later). However, its application is broader: controllers and processors can be held to account even if the data relates to people outside the EU, or if the controller/processor is outside the EU, but the data subject is inside the EU (not only citizens). So it affects anyone selling goods and services in Europe. It even applies to, for example, a US company gathering data about US citizens, if the services of an EU company are used.

The GDPR doesn't actually change the basic principles of privacy law. Rather, it serves to harmonise, clarify and reinforce existing privacy law (the rules on how we put the right to privacy into practice). For example, it clarifies what personal data is by giving examples. So it's clear that things such as IP addresses and location data obtained by smartphones count as personal data.

Anyone who handles personal data is now explicitly required to take appropriate security measures (where 'appropriate' implies reasonable in view of the sensitivity of the data, the risk of a security breach, the cost of security enhancement, etc).

Some organisations will now have to appoint a privacy officer (someone with special responsibility for privacy). However, registrars are unlikely to be covered by that requirement.

Under the GDPR, a proactive approach is required. Everyone has to be able to demonstrate that they comply with the law, e.g. by making data processing agreements with service providers, obtaining consent before distributing newsletters, or using software designed to protect privacy. The Regulation also makes it compulsory to keep records of all your personal data processing (what data you collect, who you share it with, how you store it, etc), and to make the records available to the authorities on request. (Two thirds of webinar viewers hadn't yet set up a register.)

The starting point for compliance is therefore an inventory of all the data processing going on within the organisation: what, how and why? Compliance can be broken down into three elements:

- Purpose: why are you collecting/processing personal data?
- Justification: what legitimate basis/reason do you have for collecting/processing personal data?
- Data: what personal data do you actually need to serve your justified purpose?

Applied to .nl domain registration:

- Purpose: the registration of a .nl domain name
- Justification: a contract between registrant and registrar, authorising the registrar to make the registration for the registrant
- Data: the registrant's contact details (and potentially other data)

So, although the legislation is complex, compliance doesn't have to be.

Privacy law defines three key actors:

- Data subject: person that the data relates to
- Data controller: organisation with ultimate responsibility for personal data processing; the decision-maker
- Data processor: organisation that does the actual processing (e.g. storage of contact data in a retrieval system)

Translated to domain registration:

- Data subject: the registrant/applicant
- Data controller: the registrar
- Data processor: any service provider that processes data for the registrar

However, there is considerable variety in practice: there may not be a data processor, or there may be several of them or data processors and sub-processors; there can sometimes be more than one data controller.

The GDPR clarifies a number of principles:

- Processing must be honest, transparent and careful
- Processing must serve (and not go beyond) a legitimate purpose
- The data that is processed must be kept to the minimum
- Processed data must be accurate and relevant
- Data mustn't be kept for longer than necessary
- Data has to be adequately secured
- The data controller has ultimate responsibility for the above

It's important to ask yourself whether your activities are in line with those principles. For example, you don't need a client's public service number to register a domain name for them. So, if you ask for that information, you're breaking the law by not keeping the processing to the minimum. However, some interpretation is needed: how long do you need to keep your customers' data? That is not defined in law; you have to make a reasonable judgement. The

transparency requirement implies, for example, telling clients about the categories of organisation that you share data with ("We use the services of external data centres where data is stored in accordance with processing contracts"), but not detailed and exhaustive specifications ("We use the services of companies A, B and C, who do this that and the other with the data").

Peter highlighted six justified reasons for processing personal data:

- Consent
- Contract fulfilment
- Legal obligation
- Vital interest
- Governmental responsibility
- Legitimate interest

In domain registration, the principal justification is contract fulfilment. The registrar offers a service and the registrant asks to receive that service, thus entering into a contract. It's impossible for the registrar to fulfil that contract without processing the registrant's personal data; the processing is therefore justified. However, registration involves a third party: SIDN. When a registrant asks a registrar to register a domain name, the registrant also enters into a contract with SIDN, and SIDN subsequently processes the registrant's data as well. So both the registrar and SIDN are data controllers. That implies that both the registrar and SIDN have a responsibility to fully inform the registrant, for example.

A registrar's processes must be designed with that three-way relationship in mind. When registering a name, a registrant must be made aware that data is going to SIDN as well. The registrant must have access to SIDN's terms and conditions, and the opportunity to see what SIDN is going to do with the data and why.

When a domain name is transferred, the relationship between the registrant and SIDN remains unchanged, but a new contract is agreed between the registrant and the new registrar. It must be clear to the registrant that personal data is being handed over to the new registrar, what is going to happen to that data and why. Following the transfer, the old registrar's justification for having the registrant's data ends.

When a registration is cancelled, the registrant's contracts with the registrar and SIDN both end. The original justification for data processing also ends, therefore. However, for the duration of the quarantine period, the retention of data is justified in order to enable the registrant to exercise the right to have the quarantined domain name reinstated.

3 How the Whois will change

Because .nl is a ccTLD based in the EU, registrars have been asking what SIDN is going to do to ensure compliance with the GDPR. The background to the uncertainty is tension between the GDPR's requirements (processing kept to the minimum; demonstrable purpose and

need; limitation of third-party involvement; no unrestricted access) and the interests associated with an open Whois (transparency as to registrant's identity; abuse prevention; alignment of data held by registry and registrar; public access requirement for gTLDs). ICANN is currently investigating ways of reconciling the interests associated with an open Whois with the GDPR. Until that process is complete, no action will be taken against gTLD registries that don't meet ICANN's public access requirements.

However, those requirements don't apply to ccTLDs (including .nl), whose registries are free to bring their operations into line with the new legislation without worrying about the consequences.

The GDPR doesn't have any far-reaching implications for SIDN, which has done a lot in recent years to protect registrants' privacy (opt-out; no addresses in Whois; Captcha control on Whois access; layered access to detailed info, etc).

The current situation with .nl rWhois (Whois for registrars):

- Extensive access to detailed info (99% via command line)
- Query limit = size of portfolio + 5,000
- 80% of queries relate to domain names controlled by other registrars ('extra-portfolio queries')
- No distinction between domain names you control and those you don't control

What SIDN did in response to publication of the GDPR:

- Obtained expert legal advice
- Concluded that the number of extra-portfolio queries currently permitted is disproportionate (i.e. higher than necessary for the purpose for which the data is made available)
- Concluded that the purpose of its data processing should be more precisely defined

That led to:

- Definition of new query limits and methods
- Consultation with relevant Registrars' Association committees
- Various registrars being approached about their Whois use

Planned changes:

- Distinction between domain names you control and those you don't control ('intra-' and 'extra-portfolio queries')
- New limits will apply to extra-portfolio queries (intra-portfolio queries will be unlimited)
- Limit on extra-portfolio queries: 0.75% of portfolio (minimum 25, maximum 1,000 per day)
- A registrar with 10k domain names will therefore be allowed 75 extra-portfolio queries per day
- Once limit has been reached, queries will generate error messages
- Counters will be reset overnight

- Extra-portfolio queries permitted mainly for reinstatement from quarantine, (token-free) transfers and escalations
- Longer term: extra-portfolio queries to require authorisation (e.g. token)

4 Q&A

Q: If SIDN and the registrar are both data controllers, does that imply that there's no need for a processing agreement between them?
A: Correct.

Q: If in the future a token is need for an extra-portfolio query, how will transfer escalation be possible? (Escalation is by definition something that a new registrar does when the old registrar isn't providing the transfer token.)
A: That hasn't yet been decided. SIDN might take on the task of establishing who the registrant is, or SIDN might issue tokens to escalating registrars, for example.

Q: If a registrar uses resellers, are registrar, reseller and SIDN *all* data controllers?
A: It depends on the particular relationship between the registrar and the reseller (whether both are decision-makers, or one merely acting on behalf of the other). However, the reseller is definitely a data controller if the registrant is the reseller's customer and the registration process starts with the reseller. That has implications for when the registrant is told about SIDN's involvement: if the reseller is a data controller, the reseller has a responsibility to make it clear that data will be forwarded to SIDN. In that situation, the registrar may be a data processor acting for the reseller/data controller. A registrar is therefore well advised to take a look at the contract with the reseller and decide who is giving instructions to whom about the data processing.

Q: Do the new query limits apply exclusively to the Registrar Whois? Can a registrar who has hit the daily limit still consult the public Whois?
A: Yes. Access to the public Whois is not changing.

Q: Are the General Terms and Conditions for Registrants changing?
A: Yes, changes are in the pipeline. The T&Cs for both registrars and registrants will be amended. Both GDPR-related changes and various other changes are being prepared. We will be communicating full details in due course.

Q: If the contract between registrant and registrar comes to an end, and the registrar hasn't been asked to transfer the domain name, should the registrar immediately destroy all the personal data held in connection with that registration?
A: No, the registrar shouldn't immediately destroy everything. For example, there's a requirement to retain transaction details, including the customer's details, for the tax authorities. That information has to be kept for seven years, albeit set aside for sharing exclusively with the tax authorities. The information that isn't required by the tax authorities shouldn’t necessarily be deleted immediately either. There can be reasonable grounds for retaining data for a limited period. For example, the registrar may know from experience

that, in a percentage of cases, the client does not intend to let the contract lapse and gets in touch to renew when they notice what has happened. So keeping data for a short period to facilitate renewal can be reasonable. But the policy should be clearly stated.

Q: What if the registrar has a policy of keeping data for six months after the contract has ended, but during that period the former registrant asks the registrar to delete any data that the registrar still holds? ('The right to be forgotten')
A: If a registrar gets an explicit request to delete the data, that request has to be honoured, except insofar as the law requires the registrar to retain (some) data, e.g. for the tax authorities. In the latter circumstance, the registrar has to tell the former registrant what is being kept and why.

Q: What about a reseller that works with multiple registries and registrars?
A: It is sufficient for the reseller to inform registrants that that is the case; the registries and registrars don't need to be individually named. However, if asked to do so, the reseller does need to be able to name all the organisations that data has been shared with.

Michiel thanked everyone for their participation and closed the webinar.