From: Nick Wenban-Smith
Date: Wednesday, January 10, 2018 at 10:55
To: "gdpr@icann.org" <gdpr@icann.org>
Subject: [Ext] Possible GDPR compliance models

Dear Sirs

In his 21 December 2017 blog post Göran Marby requested community feedback and suggestions before 10 January 2018 in relation to the layered access approach described as a potential interim solution in Part 3 of the Hamilton advice. Part 3 of Hamilton's legal analysis (dated 21 December 2017) focuses on personal data which is made available to the public worldwide via Whois services, and is based on ICANN's preferred option for Whois services to remain as close as possible to their current state. The background to this of course is the rapidly approaching deadline of May 2018.

Please accept this response as Nominet's feedback.

Whilst GDPR requires **all** personal data to be processed lawfully, fairly and transparently, we agree that the most pressing issue is that of Whois services. As recently confirmed by the Article 29 Data Protection Working Party in their letter to ICANN dated 11 December 2017, the unlimited publication of Whois data on the internet has been of concern to them under existing EU data protection laws since 2003. From May 2018 breaches of EU data protection law will be subject to significantly increased financial penalties, but in any event ICANN should seek to ensure that its contracted parties comply with their legal obligations. In particular ICANN should not impose on contracted parties policies which are inconsistent with national law and we are therefore very keen that as a minimum an interim solution for Whois services can be found as soon as possible.

Without prejudice to further comments in relation to the impact of GDPR on ICANN contracted parties on issues other than Whois services, our feedback is as follows:

1. We agree that registrant consent to publication of their personal data in Whois services is unlikely to be a legal ground that can be relied on. If consent to publication of personal data is a requirement for registration of a domain name, then such consent is unlikely to be regarded as freely given. In addition, there are practical difficulties in our view of obtaining consent to the standard required by GDPR in the process of registering a domain name.

2. We also agree that it is hard for ICANN to argue that publication of personal data in Whois, to the extent presently required, is necessary for the performance of a contract or other legitimate interests pursued by the controller; amongst ccTLDs there exist many current Whois models which provide acceptable provision of certain data to the public as regards domain name registrations but which do not publish personal data to the extent required of gTLDs by ICANN.

3. We start from a position that certain data in relation to a domain name registration is inherently public; in order for a website or email address to be accessed on the internet it needs to be functional for the purposes of the DNS and that requires an element of visibility to nameservers and public accessibility to anyone anywhere in the world with some basic IT knowledge. We do not therefore see any objection to the publication of domain names *per se*, together with associated technical information such as registration date and nameserver details, even if they may contain personal data – e.g. johndoe.tld. In legal terms, having the identity of a registered domain name publicly accessible for the purposes of use as a domain name and for the purposes that it was presumably registered seems to fall within the exemption that this is necessary for the performance of the registration contract.

4. As regards registrars, since these are all required to be corporate entities, we do not see any issue under GDPR with publication of registrar information associated with a domain name registration. Again whilst it is possible that associated telephone numbers, email and geographical addresses may contain personal data of registrar staff, these are essentially corporate data and registrars should be able to provide suitably generic (non personal) data for the public Whois.

5. The more complex issues arise in relation to **registrant** information which may potentially be personal data under GDPR (as well as under existing EU data protection legislation as highlighted by the Article 29 Working Party). Currently ICANN requires the publication of registrant name, contact name, a physical address, telephone number and email address. Clearly these may all comprise personal data under GDPR where the registrant is a natural person as opposed to a corporate body.

6. It appears to us that there could be two options (or a combination of the two) going forward in terms of applying an interim solution to display less registrant information in the public Whois:

a. Firstly, corporate registrations could be treated differently from those of natural persons. Corporate registrant Whois data need not in our view be modified in the light of GDPR. For natural persons the extent of their data published on the Whois service could be limited in order to bring Whois services into compliance with GDPR. For example, the Whois service for the .UK ccTLD, developed in combination with our stakeholders including the national DPA, allows natural persons to limit their Whois data to simply the registrant name in circumstances where they are not using their domain name in the course of trade. (Where a domain name is being used in the course of trade then under the e-Commerce Directive certain minimum information is in any event required to be easily, permanently and directly accessibly including name, geographic address, company registration number and email address).

b. A second option would be to limit the Whois data for **all** registrants. Given that any domain name used in the course of trade would invariably be subject to disclosure requirements such as the e-Commerce Directive, it may be that publication of registrar details and abuse contacts, in addition to simply the registrant name and geographic address only for the purposes of identification, is sufficient for law enforcement and rights holders who seek to protect the public from illegal conduct and/or enforce rights. The .UK Whois service has operated on this basis for many years now. Whilst this does not fit within any obvious exemption provided by GDPR, this bears similarities with many public registers (including for example the EU Trade Marks registry as highlighted by Hamilton).

7. In both of the options above, it should be open to third parties with a legitimate interest to seek further information from either the registry or registrar as the case may be. As regards requests for registrant information by law enforcement or rights holders in the case of the .UK ccTLD we receive on average around 15 requests per month in relation to our c. 12,000,000 registered domains. We therefore believe that while this inevitably involves a manual response and review of each request, as opposed to an automated process, this is a proportionate and workable interim solution which balances legal compliance and protection of the rights of individuals as regards their personal data, with maintaining a public Whois service to the fullest extent legally possible.

8. Certain ICANN consensus policies require use of registrant data, to be taken from the Whois. These include inter-registrar transfers (the gaining registrar is required to send confirmation of transfer request to the registrant using the details taken from the Whois) and inter-registrar transfer disputes (the losing registrar is required to

keep a copy of the Whois output). We believe that with minor modifications these processes could be changed without compromising the integrity of the process to avoid reference to Whois data. Dispute processes such as UDRP and URS already require the existing registrar or registry operator to confirm the underlying registrant data and so we do not see how these would be impacted by any changes in the public Whois output.

Yours faithfully,

Nick Wenban-Smith
General Counsel