Submitted to: EDPB@edpb.europa.eu

May 17th, 2019

Dr. Andrea Jelinek
Chairperson
European Data Protection Board

Re: Reply to public consultation – INTA - Guidelines 02/2019

Dear Dr. Jelinek:

The International Trademark Association (INTA) appreciates the opportunity to engage with the European Data Protection Board (EDPB) in response to its request for comments regarding Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.¹

INTA is committed to supporting the principles of the GDPR which ensure that appropriate weight and balance are given to the purposes and uses for collecting and processing an individual’s data and the rights of data subjects. With that understanding, INTA members recognize the link between data protection practices and brand value. The misuse of data can have adverse consequences for brands as brands are symbols of trust. Further, brands are entrusted with protecting their customers from a range of misuse and abuse including online fraud, phishing, malware and counterfeiting. In that regard, GDPR and the interests of brand owners are aligned.

As the interpretation of the provisions of GDPR evolve, INTA is pleased to provide perspective and practical information regarding the areas of concern to brand owners and consumers alike. One area of concern has been the practical application of GDPR to the contractual relationships formed under the domain name system (DNS) under the stewardship of the International Corporation for Assigned Names and Number (ICANN). We are aware that ICANN has been in continuing discussions with the EDPB and we thank the EDPB for its continued engagement as we travel the path toward an DNS framework that makes sense and works under GDPR.

Our comments below are focused on the processing of domain name registration data (also known as WHOIS data) by ICANN-accredited registrars and registries (“the Contracted Parties”) pursuant to contractual terms that flow from ICANN’s mission to ensure the stable and secure operation of the Internet’s unique identifier systems.

We note that the scope of the proposed guidelines is to provide guidance on the applicability of the legal basis for processing personal data which is set out in Article 6(1)(b) in the context of

contracts for online services, and particularly with respect to the concept of necessity as it applies to the requirement for the processing to be “necessary for the performance of a contract”.

The acquisition of a domain name in the ICANN-coordinated gTLD domain name system (DNS), whether alone or in conjunction with related services such as website design and hosting and the provision of email, is generally by means of an online service in which the registrant and an ICANN-accredited registrar are the contracting parties. This contract sets forth the terms and conditions that govern the acquisition of the domain name, as well as the ongoing rights and responsibilities of the registrant and registrar in relation to that domain name.

A number of terms in that contract are imposed by virtue of the registrant’s status as an accredited entity, which for a domain within a gTLD registry is governed by ICANN’s policies and mission. Such contractual terms may include provisions aimed at identifying who the registrant is and the accuracy of the registrant contact details provided. This serves a number of purposes, not just to ensure that the domain name is allocated and billed to the right registrant and that records can be re-created in the event of a system failure, but also, amongst other things, to ensure the stable and secure operation of the Internet’s unique identifier systems, which is a core component of ICANN’s mission. It would be helpful to understand the extent to which these purposes can be considered to be fundamental to the rationale of any contract for registrar or registry services, bearing in mind that the contractual terms required by ICANN’s accreditation framework provide the basis for registrars and registries to provide those services in the first place.

In attempting to understand the extent to which a 6(1)(b) basis applies in this context, we understand the processing must be objectively “necessary in the performance of a contract.” In this respect, it’s important to note that ICANN meets its obligations to fulfill its mission through the contractual chain by ensuring a secure, stable, resilient DNS (as specified in its Mission and Bylaws). ICANN does this by coordinating policies and enforcing its agreements to ensure that the unique network address ultimately purchased by the registrant is connected to a secure, stable, resilient network – not just any network. Registrants would not receive their end of the contractual bargain if ICANN failed to act through its contracts to prevent cybercriminals, counterfeiters, and other fraudulent actors from destabilizing the network the registrants pay to utilize. To do so, ICANN coordinates and enforces procedures like the WHOIS Accuracy Program Specification² and policies, which have been adopted by consensus within the community, like the Uniform Domain Name Dispute Resolution Proceeding (UDRP)³ and become part of ICANN’s contracted policies.

ICANN has identified specific meaning and purposes to “security”, “stability” and “resilience”.⁴ As such, they are not abstract. ICANN’s FY15-16 Identifier Systems Security, Stability and Resiliency Framework defines the elements as:

- **Security** – the capacity to protect Internet Identifier Systems and prevent misuse.

---

² [https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy](https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy)
³ [https://www.icann.org/resources/pages/help/dndr/udrp-en](https://www.icann.org/resources/pages/help/dndr/udrp-en)
• **Stability** – the capacity to ensure that Internet Identifier Systems operate as expected, and that users of these systems have confidence that the systems operate as expected or intended.

• **Resiliency** – the capacity of Internet Identifier Systems to effectively withstand, tolerate, or survive malicious attacks and other disruptive events without interruption or cessation of service.

According to the organizations that are tasked by ICANN to advise it on meeting its obligation to provide for the security, stability, and resiliency of the DNS, providing for prompt access to accurate WHOIS data is necessary to that mission. Specifically, ICANN’s Security and Stability Advisory Committee (SSAC) has submitted multiple comments in response to ICANN’s Temporary Specification for gTLD Data and the (then) ongoing EDPD advocating for access to accurate WHOIS data. For example, SSAC submitted a public comment entitled *SSAC Advisory Regarding Access to Domain Name Registration Data* on 12 December 2018 that advocated that access to domain name registration data (WHOIS data) was “essential” to that mission. The SSAC comment provided several reasons in support of that conclusion, including the fact that WHOIS data is relevant to investigation of cybercrime or fraud; mitigation of DNS abuse; the correction of technical problems and security breaches; maintenance of protective systems, such as Reputation Block Lists (RBLs) and domain name reputation scoring mechanisms; awarding digital certificates; ensuring the delivery of valid email; and research on topics such as DNS traffic, botnets, and distributed denial of service (DDoS) attacks. And the SSAC’s position in this regard is echoed in EU law as it pertains to the .eu Top Level Domain (TLD), which provides that an accessible WHOIS database is needed for the purpose of ensuring the security, stability and resilience of the .eu TLD.  

It would be beneficial if the EDPB guidelines could therefore consider and address the extent to which the 6(1)(b) basis would apply to contractual provisions required by ICANN vis a vis its agreements with Contracted Parties which are subsequently passed through to Registrants or end users. These provisions are expressly drafted to satisfy ICANN’s obligation to ensure a secure, stable, and resilient DNS. We are particularly interested in how a 6(1)(b) basis applies without conflating ICANN’s purposes with those of third parties, given that ICANN’s purpose is to provide for this third-party processing. The contracts between ICANN and its Contracted Parties cannot be separated from the Agreements with the registrants due to the nature of the domain name registration framework. We are also interested in further engagement with the EDPB on Section 3.2, Paragraph 47 *Processing for ‘fraud prevention’*, which notes that fraud prevention may involve monitoring and profiling customers, which would go beyond what is objectively necessary for the performance of a contract. We ask the EDPB to expand upon whether processing for the purposes of fraud prevention is necessarily precluded under 6(1)(b), specifically in the ICANN context where fraud prevention is necessary for the performance of the “secure, stable, resilient DNS” contractual obligation.

INTA’s members, both brand owners and those who advise them including lawyers and domain service providers, would benefit from guidelines which consider and address the need to have access to registrant data for security purposes. Such guidance would also benefit law

---


6 See Regulation (EU) 2019/517 of the European Parliament and the Council, Article 12, Section 1 “The Registry shall set up and manage, with due diligence, a WHOIS database facility for the purpose of ensuring the security, stability and resilience of the .eu TLD by providing accurate and up-to-date registration information about the domain names under the .eu TLD.”

7 See Id. Section 3 “investigation of cybercrime and fraud.” See also ICANN Bylaws, Annex G-1 and G-2 “(i) avoidance of confusion among or misleading of users”. [https://www.icann.org/resources/pages/governance/bylaws-en/#annexG1](https://www.icann.org/resources/pages/governance/bylaws-en/#annexG1).
enforcement, domain registrars, and gTLD and ccTLD registry operators. Although our comments relate specifically to draft guidelines 2/2019, there would in fact be substantial benefit for these previously-identified interested-parties and to the public as a whole for the EDPB to develop guidelines which specifically address the treatment of domain name registration data, particularly in light of repeated calls by the European Commission for the development of a model for unified access to registration data which is fully in line with EU data protection rules, in particular the GDPR, including in its letters to ICANN of 17 April and 3 May 2019 commenting on the Policy Recommendations of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data.

Thank you for your consideration of our comments and questions. If you require further information relating to this submission, please contact Lori Schulman, Senior Director, Internet Policy at lschulman@inta.org.

Sincerely,

Etienne Sanz de Acedo
Chief Executive Officer

About INTA - Founded in 1848, INTA is a global not for profit association with more than 7,200 member organizations from over 191 countries. Approximately 1,755 INTA member organizations are based in the EU and EEA. One of INTA’s goals is the promotion and of trademarks as a primary means for consumers to make informed choices regarding the products and services they purchase. INTA has also been the leading voice of trademark owners within the Internet Community, serving as a founding member of the Intellectual Property Constituency of ICANN. INTA’s Internet Committee is a group of 175 trademark owners and professionals from around the world charged with evaluating treaties, laws, regulations and procedures relating to domain name assignment, use of trademarks on the Internet, and unfair competition on the Internet, whose mission is to advance the balanced protection of trademarks on the Internet.

8 https://mm.icann.org/pipermail/comments-epdp-recs-04mar19/attachments/20190417/6f0a65b2/CommentsontheTemporarySpecificationforgTLDRegistrationDataPolicyRecommendations-0001.pdf