**REVISED RECOMMENDATIONS – FINAL REPORT EXECUTIVE SUMMARY – 1 DECEMBER 2015**

The WG has reached **FULL CONSENSUS** on the following recommendations:

I. DEFINITIONS:

1. The WG recommends the adoption of the following definitions, to avoid ambiguities surrounding the common use of certain words in the WHOIS context. The WG recommends that these recommendations be used uniformly by ICANN, including generally in relation to WHOIS beyond privacy and proxy service issues:
* ***"Privacy Service"*** means a service by which a Registered Name is registered to its beneficial user as the Registered Name Holder, but for which alternative, reliable contact information is provided by the privacy or proxy service provider for display of the Registered Name Holder's contact information in the Registration Data Service (WHOIS) or equivalent services[[1]](#footnote-1).
* ***"Proxy Service"*** is a service through which a Registered Name Holder licenses use of a Registered Name to the privacy or proxy customer in order to provide the privacy or proxy customer use of the domain name, and the Registered Name Holder's contact information is displayed in the Registration Data Service (WHOIS) or equivalent services rather than the customer's contact information.

NOTE: In relation to the definitions of a Privacy Service and a Proxy Service, the WG makes the following additional recommendation:

* + Registrars are not to knowingly[[2]](#footnote-2) accept registrations from privacy or proxy service providers who are not accredited through the process developed by ICANN. For non-accredited entities registering names on behalf of third parties, the WG notes that the obligations for Registered Name Holders as outlined in section 3.7.7 of the 2013 RAA would apply[[3]](#footnote-3).
* ***“Publication”*** means the reveal[[4]](#footnote-4) of a person’s (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details in the WHOIS system.
* ***“Disclosure”*** means the reveal of a person’s (i.e. the licensee or beneficial owner of a registered domain name) identity/contact details to a third party Requester without Publication in the WHOIS system.
* The term ***“person”*** as used in these definitions is understood to include natural and legal persons, as well as organizations and entities.
* **“Law enforcement authority”** means law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the privacy or proxy service provider is established or maintains a physical office. This definition is based on Section 3.18.2 of the 2013 Registrar Accreditation Agreement, which provision spells out a registrar’s obligation to maintain a point of contact for, and to review reports received from, law enforcement authorities[[5]](#footnote-5); as such, the WG notes that its recommendation for a definition of “law enforcement authority” in the context of privacy and proxy service accreditation should also be updated to the extent that, and if and when, the corresponding definition in the RAA is modified.
* ***“Relay”***, when used in the context of a request to a privacy or proxy service provider from a Requester, means to forward the request to, or otherwise notify, the privacy or proxy service customer that a Requester is attempting to contact the customer.
* ***“Requester”***, when used in the context of Relay, Disclosure or Publication, including in the Illustrative Disclosure Framework described in Annex B, means an individual, organization or entity (or its authorized representatives) that requests from a privacy or proxy service provider either a Relay, or Disclosure or Publication of the identity or contact details of a customer, as the case may be.
* ***“Affiliate”***, when used in this Final Report in the context of the relationship between a privacy or proxy service provider and an ICANN-accredited registrar, means a privacy or proxy service provider that is Affiliated with such a registrar, in the sense that word is used in the [2013 RAA](https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en). Section 1.3 of the 2013 RAA defines an “Affiliate” as a person or entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, the person or entity specified.

II. NO DISTINCTION IN TREATMENT; WHOIS LABELING REQUIREMENTS; VALIDATION & VERIFICATION OF CUSTOMER DATA:

1. Privacy and proxy services (“P/P services”) are to be treated the same way for the purpose of the accreditation process.
2. The status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether P/P services are available to the registrant. Fundamentally, P/P services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals. Further, P/P registrations should not be limited to private individuals who use their domains for non-commercial purposes.
3. To the extent that this is feasible, domain name registrations involving P/P service providers should be clearly labelled as such in WHOIS[[6]](#footnote-6).
4. P/P customer data is to be validated and verified in a manner consistent with the requirements outlined in the [WHOIS Accuracy Program Specification](https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy) of the 2013 RAA (as may be updated from time to time). In the cases where a P/P service provider is Affiliated with a registrar and that Affiliated registrar has carried out validation and verification of the P/P customer data, re-verification by the P/P service provider of the same, identical, information should not be required.

MANDATORY PROVISIONS TO BE INCLUDED IN PROVIDER TERMS OF SERVICE & MINIMUM REQUIREMENTS TO BE COMMUNICATED TO CUSTOMERS:

1. All rights, responsibilities and obligations of registrants and P/P service customers as well as those of accredited P/P service providers need to be clearly communicated in the P/P service registration agreement, including a provider’s obligations in managing those rights and responsibilities and any specific requirements applying to transfers and renewals of a domain name. In particular, all accredited P/P service providers must disclose to their customers the conditions under which the service may be terminated in the event of a transfer of the domain name, and how requests for transfers of a domain name are handled.
2. All accredited P/P service providers must include on their websites, and in all Publication and Disclosure-related policies and documents, a link to either a request form or list containing a set of specific, minimum, mandatory criteria, or an equivalent list of such criteria, that the provider requires in order to determine whether or not to comply with third party requests, such as for the Disclosure or Publication of customer identity or contact details.
3. All accredited P/P service providers must publish their terms of service (e.g. on their websites), which, in addition to other mandatory provisions recommended by the WG, should at a minimum include the following elements in relation to Disclosure and Publication:
* Clarification of when those terms refer to Publication requests (and their consequences) and when they refer to Disclosure requests (and their consequences). The WG further recommends that accredited providers expressly include a provision in their terms of service explaining the meaning and consequences of Publication.
* The specific grounds upon which a customer’s details may be Disclosed or Published or service suspended or terminated, including Publication in the event of a customer’s initiation of a transfer of the underlying domain name[[7]](#footnote-8). In making this recommendation, the WG noted the changes to be introduced to the [Inter Registrar Transfer Policy](https://www.icann.org/resources/pages/registrars/transfers-en) (“IRTP”) in 2016[[8]](#footnote-9), where following a Change of Registrant[[9]](#footnote-10), a registrar is required to impose a 60-day inter-registrar transfer lock.
* Clarification as to whether or not a customer: (1) will be notified when a provider receives a Publication or Disclosure request from a third party; and (2) may opt to cancel its domain registration prior to and in lieu of Publication or Disclosure. However, accredited P/P service providers that offer this option should nevertheless expressly prohibit cancellation of a domain name that is the subject of a UDRP proceeding.
* Clarification that a Requester will be notified in a timely manner of the provider’s decision: (1) to notify its customer of the request; and (2) whether or not the provider agrees to comply with the request to Disclose or Publish. This should also be clearly indicated in all Disclosure or Publication related materials.
1. In addition, the WG recommends the following as best practices for accredited P/P service providers[[10]](#footnote-13):
* P/P service providers should facilitate and not obstruct the transfer[[11]](#footnote-14), renewal or restoration of a domain name by their customers, including without limitation a renewal during a Redemption Grace Period under the [Expired Registration Recovery Policy](https://www.icann.org/resources/pages/errp-2013-02-28-en) and transfers to another registrar.
* P/P service providers should use commercially reasonable efforts to avoid the need to disclose underlying customer data in the process of renewing, transferring or restoring a domain name.
* P/P service providers should include in their terms of service a link or other direction to the ICANN website (or other ICANN-approved online location such as the provider’s own website) where a person may look up the authoritative definitions and meanings of specific terms such as Disclosure or Publication.

CONTACTABILITY & RESPONSIVENESS OF PRIVACY & PROXY SERVICE PROVIDERS:

1. ICANN should publish and maintain a publicly accessible list of all accredited P/P service providers, with all appropriate contact information. Registrars should be advised to provide a web link to P/P services run by them or their Affiliates as a best practice. P/P service providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program[[12]](#footnote-15).
2. P/P service providers must maintain a point of contact for abuse reporting purposes. In this regard, a “designated” rather than a “dedicated” point of contact will be sufficient, since the primary concern is to have one contact point that third parties can go to and expect a response from. For clarification, the WG notes that as long as the requirement for a single point of contact can be fulfilled operationally, it is not mandating that a provider designate a specific individual to handle such reports.
3. P/P service providers should be fully contactable, through the publication of contact details on their websites in a manner modelled after Section 2.3 of the 2013 RAA [Specification on Privacy and Proxy Registrations](https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#privacy-proxy), as may be updated from time to time.
4. Requirements relating to the forms of alleged malicious conduct to be covered by the designated published point of contact at an ICANN-accredited P/P service provider should include a list of the forms of malicious conduct to be covered. These requirements should allow for enough flexibility to accommodate new types of malicious conduct. By way of example, Section 3 of the Public Interest Commitments (PIC) Specification[[13]](#footnote-16) in the New gTLD Registry Agreement or Safeguard 2, Annex 1 of the GAC’s Beijing Communique[[14]](#footnote-17) could serve as starting points for developing such a list.
5. The designated point of contact for a P/P service provider should be capable and authorized to investigate and handle abuse reports and information requests received.

STANDARD FORM & REQUIREMENTS FOR ABUSE REPORTING & INFORMATION REQUESTS:

1. A uniform set of minimum mandatory criteria that must be followed for the purpose of reporting abuse and submitting requests (including requests for the Disclosure of customer information) should be developed. Forms that may be required by individual P/P service providers for this purpose should also include space for free form text[[15]](#footnote-18). P/P service providers should also have the ability to “categorize” reports received, in order to facilitate responsiveness. P/P service providers must also state the applicable jurisdiction in which disputes (including any arising under the Illustrative Disclosure Framework in Annex B) should be resolved on any forms used for reporting and requesting purposes.

RELAYING (FORWARDING) OF THIRD PARTY REQUESTS:

1. Regarding Relaying of Electronic Communications[[16]](#footnote-19):
* All communications required by the RAA and ICANN Consensus Policies must be Relayed.
* For all other electronic communications, P/P service providers may elect one of the following two options:
	+ 1. Option #1: Relay all electronic requests received (including those received via emails and via web forms), but the provider may implement commercially reasonable safeguards (including CAPTCHA) to filter out spam and other forms of abusive communications, or
		2. Option #2: Relay all electronic requests received (including those received via emails and web forms) from law enforcement authorities and third parties containing allegations of domain name abuse (i.e. illegal activity)
* In all cases, P/P service providers must publish and maintain a mechanism (e.g. designated email point of contact) for Requesters to contact to follow up on or escalate their original requests.
1. Regarding Further Provider Actions When There Is A Persistent Delivery Failure of Electronic Communications:
* All third party electronic requests alleging abuse by a P/P service customer will be promptly Relayed to the customer. A Requester will be promptly notified of a persistent failure of delivery[[17]](#footnote-20) that a P/P service provider becomes aware of.
* The WG considers that a “persistent delivery failure” will have occurred when an electronic communications system abandons or otherwise stops attempting to deliver an electronic communication to a customer after a certain number of repeated or duplicate delivery attempts within a reasonable period of time. The WG emphasizes that such persistent delivery failure, in and of itself, is not sufficient to trigger further provider obligation or action in relation to a relay request unless the provider also becomes aware of the persistent delivery failure.
* As part of an escalation process, and when the above-mentioned requirements concerning a persistent delivery failure of an electronic communication have been met, the provider should upon request Relay a further form of notice to its customer. A provider should have the discretion to select the most appropriate means of Relaying such a request. A provider shall have the right to impose reasonable limits on the number of such requests made by the same Requester for the same domain name.
* When a service provider becomes aware of a persistent delivery failure to a customer as described herein, that will trigger the P/P service provider’s obligation to perform a verification/re-verification (as applicable) of the customer’s email address(es), in accordance with the WG’s recommendation that customer data be validated and verified in a manner consistent with the WHOIS Accuracy Specification of the 2013 RAA (see Recommendation #5, above, and the background discussion under Category B, Question 2 in Section 7, below).
* However, these recommendations shall not preclude a P/P service provider from taking any additional action in the event of a persistent delivery failure of electronic communications to a customer, in accordance with its published terms of service.

DISCLOSURE OR PUBLICATION OF A CUSTOMER’S IDENTITY OR CONTACT DETAILS:

1. Regarding Disclosure and Publication, the WG agreed that none of its recommendations should be read as being intended to alter (or mandate the alteration of) the prevailing practice among P/P service providers to review requests manually or to facilitate direct resolution of an issue between a Requester and a P/P service customer. It also notes that disclosure of at least some contact details of the customer may in some cases be required in order to facilitate such direct resolution. In relation to Publication that is subsequently discovered to be unwarranted, the WG believes that contractual agreements between providers and their customers and relevant applicable laws will govern, and are likely to provide sufficient remedies in such instances.
2. The WG has developed an illustrative Disclosure Framework to apply to Disclosure requests made to P/P service providers by intellectual property (i.e. trademark and copyright) owners. The proposal includes requirements concerning the nature and type of information to be provided by a Requester, non-exhaustive grounds for refusal of a request, and the possibility of neutral dispute resolution/appeal in the event of a dispute. The WG recommends that a review of this Disclosure Framework be conducted at an appropriate time after the launch of the program and periodically thereafter, to determine if the implemented recommendations meet the policy objectives for which they were developed. Such a review might be based on the non-exhaustive list of guiding principles developed by the GNSO’s Data and Metrics for Policy Making (DMPM) WG, as adopted by the GNSO Council and ICANN Board. As noted by the DMPM WG, relevant metrics could include industry sources, community input via public comment or surveys or studies. In terms of surveys (whether or providers, customers or requesters), data should be anonymized and aggregated. Please refer to Annex B for the full Disclosure Framework.
3. Although the WG has reached consensus on an illustrative Disclosure Framework for handling requests from intellectual property (i.e. trademark and copyright) rights-holders, it has not developed a similar framework or template that would apply to other Requesters, such as LEA or anti-abuse and consumer protection groups. The WG is aware that certain concerns, such as the need for confidentiality in relation to an on-going LEA investigation, may mean that different considerations would apply to any minimum requirements that might be developed for such a framework. In this regard, in its Initial Report the WG had sought community feedback on specific concerns relating to the handling of LEA requests, such as whether or not providers should be mandated to comply with them. Based on input received, the WG recommends that accredited P/P service providers should comply with express requests from LEA not to notify a customer where this is required by applicable law. However, this recommendation is not intended to prevent providers from either voluntarily adopting more stringent standards or from cooperating with LEA. In the event that a Disclosure Framework is eventually developed for LEA requests, the WG recommends that the Framework expressly include requirements under which at a minimum: (a) the requester agrees to comply with all applicable data protection laws and to use any information disclosed to it solely for the purpose to determine whether further action on the issue is warranted, to contact the customer, or in a legal proceeding concerning the issue for which the request was made; and (b) exempts Disclosure where the customer has provided, or the P/P service provider has found, specific information, facts, and/or circumstances showing that Disclosure will endanger the safety of the customer.

DEACCREDITATION & ITS CONSEQUENCES:

1. Regarding de-accreditation of a P/P service provider:

The WG reiterates its previous observation that increased risks to a customer’s privacy may be involved when a customer is dealing with a P/P service provider who, even if accredited by ICANN, is not Affiliated with an ICANN-accredited registrar. De-accreditation was noted as one topic where additional problems may arise. The WG therefore recommends that the following general principles be adopted and followed when a more detailed P/P service de-accreditation process is developed during implementation. As with transfers of domain names that occur other than as a result of de-accreditation of a P/P service provider, these principles are based on the WG’s belief that customer privacy should be a paramount concern. As such, reasonable safeguards to ensure that a customer’s privacy is adequately protected in the course of de-accreditation of a customer’s P/P service provider – including when transfer of a customer’s domain name or names is involved – should be integral to the rules governing the de-accreditation process.

Principle 1: A P/P service customer should be notified in advance of de-accreditation of a P/P service provider. The WG notes that the current practice for registrar de-accreditation involves the sending of several breach notices by ICANN Compliance prior to the final step of terminating a registrar’s accreditation. While P/P service provider de-accreditation may not work identically to that for registrars, the WG recommends that ICANN explore practicable ways in which customers may be notified during the breach notice process (or its equivalent) once ICANN issues a termination of accreditation notice but before the de-accreditation becomes effective. . The WG recommends that de-accreditation become effective for existing customers 30 days after notice of termination. The WG notes that, in view of the legitimate need to protect many customers’ privacy, the mere publication of a breach notice on the ICANN website (as is now done for registrar de-accreditation) may not be sufficient to constitute notification.

Principle 2: Each step in the de-accreditation process should be designed so as to minimize the risk that a customer’s personally identifiable information is made public.

Principle 3: The WG notes that the risk of inadvertent publication of a customer’s details in the course of de-accreditation may be higher when the provider in question is not Affiliated with an ICANN-accredited registrar. As such, implementation design of the de-accreditation process should take into account the different scenarios that can arise when the provider being de-accredited is, or is not, Affiliated with an ICANN-accredited registrar.

In addition to the three principles outlined above, the WG recommends specifically that, where a Change of Registrant (as defined under the IRTP) takes place during the process of de-accreditation of a proxy service provider, a registrar should lift the mandatory 60-day lock at the express request of the beneficial user, provided the registrar has also been notified of the de-accreditation of the proxy service provider[[18]](#footnote-21).

**1.3.2. ADDITIONAL GENERAL RECOMMENDATIONS**

In addition to the recommendations it developed for each of its Charter questions, the WG also recommends that the following general principles be adopted as part of the P/P service provider accreditation program.

First, the next review of the IRTP should include an analysis of the impact on P/P service customers, to ensure that adequate safeguards are in place as regards P/P service protection when domain names are transferred pursuant to an IRTP process. Where a P/P service customer initiates a transfer of a domain name, the WG recognizes that a registrar should have the same flexibility that it has currently to reject incoming transfers from any individual or entity, including those initiated by accredited P/P services. Nevertheless, the WG recommends that, in implementing those elements of the P/P service accreditation program that pertain to or that affect domain name transfers and in addition to its specific recommendations contained in this Final Report, ICANN should perform a general “compatibility check” of each proposed implementation mechanism with the then-current IRTP.

Secondly, the WG recommends that ICANN develop a public outreach and educational program for registrars, P/P service providers and customers (including potential customers) to inform them of the existence, launch and features of the P/P service accreditation program.

Thirdly, the WG recommends that providers should be required to maintain statistics on the number of Publication and Disclosure requests received and the number honored, and provide these statistics in aggregate form to ICANN for periodic publication. The data should be aggregated so as not to create a market where nefarious users of the domain name system are able to use the information to find the P/P service that is least likely to make Disclosures.

Finally, the WG has concluded that the registrar accreditation model with its multiple steps, governed by the RAA, may not be entirely appropriate for P/P services; however, it is a useful starting point from which relevant portions may be adapted to apply to P/P service providers. The implications of adopting a particular accreditation model will need to be worked out as part of the implementation of its policy recommendations, if adopted.

1. The definitions of Privacy Service and Proxy Service reflect those in the 2013 RAA. In this context, the 2013 RAA also defines “Registered Name” as a domain name within the domain of a gTLD, about which a gTLD Registry Operator (or an Affiliate or subcontractor thereof engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance, and “Registered Name Holder” is defined as the holder of a Registered Name. [↑](#footnote-ref-1)
2. In this context, “knowingly” refers to actual knowledge at the time that the registration is submitted to the registrar. As implementation guidance, this knowledge would normally be obtained through a report to the registrar from ICANN or a third party. [↑](#footnote-ref-2)
3. Section 3.7.7.3 of the 2013 RAA reads as follows: “Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name.” [↑](#footnote-ref-3)
4. As the single word “reveal” has been used in the WHOIS context to describe the two distinct actions that the WG has defined as “Disclosure” and “Publication”, the WG is using “reveal” within its definitions as part of a more exact description, to clarify which of the two meanings would apply in any specific instance. The rest of this Initial Report generally uses the terms “Disclosure” and “Publication” to refer to the relevant specific aspect of a “reveal”. [↑](#footnote-ref-4)
5. See https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en. [↑](#footnote-ref-5)
6. While this may be possible with existing fields, the WG has also explored the idea that the label might also be implemented by adding another field to WHOIS, and is aware that this may raise certain questions that should be appropriately considered as part of implementation. For clarity, references to “WHOIS” in this Final Report are to the current globally accessible gTLD Registration Directory Service as well as any successors or replacements thereto. [↑](#footnote-ref-6)
7. The WG believes there should be no mandatory restriction on providers being able to terminate service to a customer on grounds stated in the terms of service, subject to any other specific limitation that may be recommended in this report by the WG. The WG notes that it is probably not possible to create a general policy that would in all cases prevent Publication via termination of service where the customer is ultimately shown to have been innocent (i.e. not in breach). [↑](#footnote-ref-8)
8. [↑](#footnote-ref-9)
9. Defined as a material, i.e. non-typographical, change to either the registrant name, organization or email address. [↑](#footnote-ref-10)
10. The WG recognizes that implementation of these recommendations may involve the development of new procedures. [↑](#footnote-ref-13)
11. See also the WG’s observations below under Recommendation #22 regarding the additional risks and challenges that may arise when the P/P service provider is independent of (i.e. not Affiliated with) an ICANN-accredited registrar, and which may be of particular concern in relation to transfers and de-accreditation issues. [↑](#footnote-ref-14)
12. The WG discussed, but did not reach consensus on, the possibility of requiring a registrar to also declare its Affiliation (if any) with a P/P service provider. [↑](#footnote-ref-15)
13. See <http://newgtlds.icann.org/en/applicants/agb/agreement-approved-20nov13-en.pdf>; Section 3 provides that “Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.” [↑](#footnote-ref-16)
14. See <https://www.icann.org/en/system/files/correspondence/gac-to-board-11apr13-en.pdf>; Safeguard 2, Annex 1 provides that ““Registry operators will ensure that terms of use for registrants include prohibitions against the distribution of malware, operation of botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law.” [↑](#footnote-ref-17)
15. With the specific exception of Disclosure requests from intellectual property rights holders (see Recommendation #19 below), the WG discussed but did not finalize the minimum elements that should be included in such a form in relation to other requests and reports. The WG notes that this recommendation is not intended to prescribe the method by which a provider should make this form available (e.g. through a web-based form) as providers should have the ability to determine the most appropriate method for doing so. [↑](#footnote-ref-18)
16. The WG agrees that emails and web forms would be considered “electronic communications” whereas human-operated faxes would not. The WG recommends that implementation of the concept of “electronic communications” be sufficiently flexible to accommodate future technological developments. [↑](#footnote-ref-19)
17. The WG notes that failure of “delivery” of a communication is not to be equated with the failure of a customer to “respond” to a request, notification or other type of communication. [↑](#footnote-ref-20)
18. The WG notes that the new changes to the IRTP give a registrar the discretion to lift the lock at the beneficial user’s request, and that no specific exceptions were created at the time the policy was reviewed. [↑](#footnote-ref-21)