PPSAI Consensus Policy Requirements for Privacy and Proxy (P/P) Service Providers (19 May 2026)

Purpose: The aim of this document is to ensure there is a clear understanding of the specific policy requirements relating to P/P service providers that would be placed on registrars in order to faithfully implement the PPSAI recommendations.

An understanding of these requirements will be used to help determine how entities providing their own P/P services are accounted for in the PPSAI Consensus Policy and guide the continued drafting of policy language.

List of requirements: The thirteen requirements outlined in this document are limited to the requirements relating to P/P service providers for the purposes of this discussion and do not reflect all PPSAI Final Report requirements which may be placed on ICANN or the policy itself.

Note: Some of these requirements are part of existing obligations that were instituted as a temporary measure under the P/P Specification[1] in the RAA prior to implementation of the PPSAI recommendations.

[1] During the 2013 RAA negotiations, ICANN and the Registrars' negotiating team had agreed that a number of interim protections would be in place for P/P services offered through Registrars or their Affiliates. These interim protections require that information be made available on matters such as abuse reporting processes and the circumstances under which a provider will relay third party communications to a P/P customer, terminate a customer's service, and publish a customer's details in WHOIS. While these are not necessarily comprehensive in terms of the terms and protections that can be put in place for accredited P/P service providers, these interim protections were intended to provide a more responsible marketplace until a formal accreditation program is developed by ICANN. (PDP WG Final Report, pgs. 25-26.)

List of PPSAI Consensus Policy Requirements for P/P Service Providers

List of P/P Service Providers	
Requirement #1:	ICANN list of accredited P/P service providers
PDP WG Recommendation 10:	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.
Related requirement(s):	RAA Registrar Information Specification (Sections 24-5).
Current implementation approach:	• ICANN will publish a list of accredited P/P service providers via mechanism TBD. • Registrars will be required to notify ICANN of P/P service providers that offer services shielding registered names sponsored by the registrar.

Registration Data Directory Services	
Requirement #2:	Labeling
PDP WG Recommendation 4:	To the extent feasible, domain name registrations involving P/P service providers should be clearly labelled as such in WHOIS.
Related requirement(s):	None.
Current implementation approach:	• Registered names that are shielded (to be defined in policy) by a P/P service must be labeled in the Registration Data Directory Services (RDDS) via a mechanism implemented by ICANN (exact mechanism TBD). • Registrar is responsible for the provision of registrar services for all registered names that the registrar sponsors, being performed in compliance with the agreement, regardless of whether the registrar services are provided by registrar or a third party, including a reseller.

Customer Data Validation and Verification	
Requirement #3:	Customer data validation/verification
PDP WG Recommendation 5:	P/P customer data is to be validated and verified in a manner consistent with the requirements outlined in the WHOIS Accuracy Program Specification 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, reverification by the P/P service provider of the same, identical, information should not be required.
Related requirement(s):	The Registrar Accreditation Agreement's RDDS Accuracy Program Specification provides an established framework for validation and verification of registrant contact data that can be leveraged for validation and verification of customer contact data.
Current implementation approach:	• Contact data pertaining to P/P customers must be validated and verified in the same manner as registrant data specified in the RAA's RDDS Accuracy Program Specification.

Privacy and Proxy Service Agreement	
Requirement #4:	Privacy/Proxy service agreement
PDP WG Recommendation 6:	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.
Related requirement(s):	Specification on Privacy & Proxy Registrations provides some related language that can be leveraged.
Current implementation approach:	• P/P service providers must enter into an agreement with each customer that sets out all rights and obligations, including specific required provisions listed in Final Report.

P/P Service Provider Identity, Contact Information, and Terms of Service	
Requirement #5:	Publication of P/P terms of service
PDP WG	All accredited P/P service providers must publish their terms of service,

Recommendation 8:	including pricing (e.g. on their websites). In addition to other mandatory provisions recommended by the WG, the terms 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[16]. In making this recommendation, the WG noted the changes to be introduced to the Inter Registrar Transfer Policy ("IRTP") in 2016, where following a Change of Registrant[17] 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. [16] 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). [17] This is defined as a material, i.e. non-typographical, change to either the registrant name, organization or email address (or in the absence of an email contact, the administrative contact listed for the registrant).
Related requirement(s):	RAA Specification on Privacy & Proxy Registrations 2.1- P/P Provider shall publish the terms and conditions of its service (including pricing), on its website and/or Registrar's website.
Current implementation approach:	● P/P service providers must publish their terms of service on the P/P service provider and/or registrar website.

Requirement #6:	Publication of P/P service provider contact information
PDP WG Recommendation 12:	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, as may be updated from time to time.
Related requirement(s):	RAA Specification on Privacy & Proxy Registrations 2.3 Disclosure of Identity of P/P Provider. P/P Provider shall publish its business contact information on its website and/or Registrar's website.
Current implementation approach:	• P/P service provider must publish its business contact information on its website and/or registrar's website.

Abuse Reporting	
Requirement #7:	P/P service provider abuse reporting contact
PDP WG Recommendation 11:	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.
Related requirement(s):	RAA Specification on Privacy & Proxy Registrations 2.2 Abuse/Infringement Point of Contact. P/P service providers shall publish a point of contact for third parties wishing to report abuse or infringement of trademarks (or other rights).
Current implementation approach:	• P/P service providers must designate a contact to receive and act upon reports of abuse.

Requirement #8:	P/P service provider Abuse Contact (list)
PDP WG Recommendation 13:	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[21] in the New gTLD Registry

	Agreement or Safeguard 2, Annex 1 of the GAC's Beijing Communique22 could serve as starting points for developing such a list. [21] 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."
Related requirement(s):	Registry Agreement.
Current implementation approach:	● Along with publication of abuse contact information, P/P service provider must identify what types of abuse the abuse contact is authorized to act upon.

Requirement #9:	Point of contact authorization for investigation and abuse reports
PDP WG Recommendation 14:	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.
Related requirement(s):	RAA 3.18 - Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.
Current implementation approach:	● P/P service provider abuse contact must investigate and handle abuse reports.

Relay of Communications to Privacy and Proxy Service Customers	
Requirement #10:	Relay of communications to customers
PDP WG Recommendation 16:	Regarding Relaying of Electronic Communications: ● 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: ○ 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 ○ 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.
Related requirement(s):	Reg Data policy, Section 11 (Log Files).
Current implementation approach:	● P/P service providers must relay communications (as specified). ● Contact data published by a P/P service provider must include a mechanism to escalate/follow up on requests. ● P/P service provider must retain logs of relay requests/relay attempts.

Requirement #11:	Persistent delivery failures
PDP WG Recommendation 17:	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[25] 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 the WG's 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. [25] 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.
Related requirement(s):	2013 RAA: RDDS Accuracy Program Specification.
Current implementation approach:	● In the course of relaying a communication to a customer (as required by Policy) P/P service provider must take certain actions when there is a persistent delivery failure. ○ Must verify/re-verify contact information ○ Must relay to additional customer contact point if requested by requestor

Data Retention and Escrow	
Requirement #12:	Carry-over of registrar data escrow requirement for P/P customer data
Current requirement in the RAA: ● 3.4 Retention of Registered Name Holder and Registration Data ● P/P Specification under Section 2: Registrar Obligations	RAA Subsection 3.4.1.5: the name, postal address, e-mail address, and voice telephone number provided by the customer of any privacy service or licensee of any proxy registration service, in each case, offered or made available by Registrar or its Affiliates in connection with each registration. Effective on the date that ICANN fully implements a Proxy Accreditation Program established in accordance with Section 3.14, the obligations under this Section 3.4.1.5 will cease to apply as to any specific category of data (such as postal address) that is expressly required to be retained by another party in accordance with such Proxy Accreditation Program. RAA Section 3.6: Registrar must include data specified above [RAA 3.4.1.5] in data escrow deposits. P/P Specification Subsection 2.5: Escrow of P/P Customer Information. Registrar shall include P/P Customer contact information in its Registration Data Escrow deposits required by Section 3.6 of the Agreement. P/P Customer Information escrowed pursuant to this Section 2.5 of this Specification may only be accessed by ICANN in the

	event of the termination of the Agreement or in the event Registrar ceases business operations.
Related requirement(s):	None.
Current implementation approach:	● Registrar must include P/P customer contact data for registered names sponsored by the registrar in the registrar's data escrow deposits required per Section 3.6 of the RAA.

Disclosure and Publication	
Requirement #13:	Publication of P/P request policies and procedures
PDP WG Recommendation 7:	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 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.
Related requirement(s):	Reg Data Policy, Section 10 (Disclosure Requests) and potentially RDRS disclosure policy language.
Current implementation approach:	Policies and procedures of P/P service providers must be published on the P/P service provider and/or registrar website.