Lawful Basis under GDPR:

6.1 (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

6.1 (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

6.1 (c) processing is necessary for compliance with a legal obligation to which the controller is subject[1];

6.1 (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

6.1 (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6.1 (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Note: please focus your input on the lawful basis and possible differences that may apply. General input on the language from the zero draft for the different building blocks will be discussed separately.

[1] The advice from Bird & Bird notes that a controller generally cannot rely on Article 6(1)(c) of the GDPR to disclose personal data to a law enforcement authority outside of its jurisdiction; the controller may, however, be able to show a legitimate interest under Article 6(1)(f) to disclose the personal data. The full response to the question may be found here: ICANN-EPDP - Q4 - 9th September 2019.

	Building Block a) (Criteria/content of requests) – Current language: The EPDP Team recommends that, consistent with the EPDP Phase 1 recommendations, each SSAD request must include, at a minimum, the following information: i. Identification of and information about the requestor (including, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant); ii. Information about the legal rights of the requestor and specific rationale and/or justification for the request, (e.g. What is the basis or reason for the request; Why is it necessary for the requestor to ask for this data?); iii. Affirmation that the request is being made in good faith; iv. A list of data elements requested by the requestor and why this data is limited to the need; v. Agreement to process lawfully any data received in response to the request. *Please specify what additional information needs to be provided or does not need to be provided if it concerns a disclosure request for which the controller discloses under the following lawful basis:*
6.1(a) Consent	No additional information required assuming disclosure is within the scope of a valid consent lawfully obtained by the Controller to disclose the data subject's personal data. Note that practically speaking, where consent has been obtained, the data should be available as part of a general public query.
6.1(b) performance of contract	Requests by a third-party for disclosure not generally appropriate under 6.1(b) since the performance of the contract is between the Contracted Party and the data subject.
6.1(c) Legal obligation	(i) Reference to the specific legal obligation or authority that the requestor is acting under (e.g., legislation, regulations, MLATs, etc.); (ii) the specific jurisdiction of the requestor; (iii) reference to the specific legal obligation that the disclosing controller is subject to.
6.1(d) Vital interests	Specific statement, with relevant and sufficient grounding evidence, on the vital interests requiring disclosure (e.g., essential for the life of the data subject or that of another natural person) and that the processing cannot be manifestly based on another legal basis.
6.1(e) Public Interest	Not applicable. The advice from Bird & Bird has confirmed that 6.1 (e) requires that "the task or authority in question must be laid down by EU or Member State law." Given that no applicable legal authority exists for ICANN or the Contracted Parties to act in the public interest, we should remove this legal basis from consideration in our policy discussions.
6.1(f) Legitimate Interest	Specific detailed description of a real and present (not vague and speculative) interest in disclosure of the data subject's personal data. Requestors should have capability to add supporting documentation to demonstrate their interest in the data.

Building block d) Acceptable Use Policy (Requestor)

The EPDP Team recommends that the following requirements are applicable to the requestor and must be confirmed & enforced by [TBC]:

i. Must only request data from the current RDS data set (no data about the domain name registration's history);
ii. Must provide representations with each unique request for data of its corresponding purpose and legal basis for their processing which will be subject to auditing (no bulk access);
iii. Must only use the data for the purpose requested;
iv. Must handle the data subject's personal data in compliance with data protection laws such as GDPR;
v. Must provide representations about use of requested data which will be subject to auditing;
vi. [Other]

Please specify what additional requirements need to apply or do not apply if it concerns a disclosure request for which the controller discloses under the following lawful basis:

6.1(a) Consent	Acceptable use policy should be uniform regardless of legal basis. Much of the applicable elements for a GDPR compliant AUP will be included in the required Standard Contractual Clauses (per Bird & Bird advice)
6.1(b) performance of contract	See response to 6.1(a) above.
6.1(c) Legal obligation	See response to 6.1(a) above.
6.1(d) Vital interests	See response to 6.1(a) above.
6.1(e) Public Interest	Not applicable. See response on pg. 2 above.
6.1(f) Legitimate Interest	See response to 6.1(a) above.

	Building block g) (Response requirements / expectations, including timeline/SLAs) Consistent with the EPDP Phase 1 recommendations, the EPDP Team recommends that [TBC] The EPDP Team recommends that if the entity disclosing the data determines that disclosure would be in violation of applicable laws AND result in inconsistency with these policy recommendations, the entity disclosing the data must document the rationale and communicate this information to the requestor and ICANN Compliance (if requested). If a requestor is of the view that the entity disclosing the data's response is not consistent with these policy recommendations or applicable data protection legislation, a complaint should be filed with ICANN Compliance or the relevant data protection authority. *Please specify what additional requirements need to apply or do not apply if it concerns a disclosure request for which the controller discloses under the following lawful basis:*
6.1(a) Consent	It is reasonable for a Contracted Party to reject a request if the requested data is beyond the scope of a valid consent lawfully obtained by the Controller to disclose the data subject's personal data. Note that practically speaking, where consent has been obtained, the data should be available as part of a general public query.
6.1(b) performance of contract	It is reasonable for a Contracted Parties to reject a request if the requested disclosure if not necessary for the performance of the contract between the Contracted Party and the data subject.
6.1(c) Legal obligation	Novel legal obligations will likely require the most intensive review given the potential complexity per request.
6.1(d) Vital interests	It is reasonable for a Contracted Party to reject a request if the vital interest is not sufficiently specific or if there is another legal means for appropriate processing of the data.
6.1(e) Public Interest	Not applicable. See response on pg. 2 above.
6.1(f) Legitimate Interest	Contracted Parties may reject requests if, upon performing the balancing test, the Contracted Party determines that the data subject's rights outweigh the interests of the requestors. A requestor may provide additional information to assist with a further balancing test with the recognition that there is no formula that will specifically guarantee disclosure. We should defer to the Contracted Parties judgment and discretion in performing the balancing test.

Comment: ICANN Compliance has a role in enforcing the policy against Contracted Parties who fail to respond at all (or within agreed SLAs) to legitimate requests for disclosure, but has no role in reviewing or assessing the substantive rationale of Contracted Parties who, based on their own assessment of applicable laws, declines to provide data to a third-party requestor. Any complaints regarding the substance of a response should be filed with the appropriate data protection authority, not ICANN Compliance.

Building block h) (Acceptable Use Policy)

The EPDP Team recommends that the following requirements are applicable to the entity disclosing the data and must be confirmed & enforced by [TBC]:

a) Must only supply the necessary data requested by the requestor;
b) Must return current data in response to a request;
c) Must process data in compliance with data protection laws such as GDPR;
d) Must log requests;
e) Where applicable, must define and perform a balancing test before processing the data. The data subject should be able to challenge –with proper substantiation- the balancing test with rights to object and to erasure;
f) Must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per relevant data protection laws such as GDPR;
g) Any system designed for disclosing of non-public registration data to Law Enforcement Authorities must include a mechanism for implementing the need for confidentiality for ongoing investigations.

Please specify what additional requirements need to apply or do not apply if it concerns a disclosure request for which the controller discloses under the following lawful basis:

6.1(a) Consent	No further requirements.
6.1(b) performance of contract	No further requirements.
6.1(c) Legal obligation	No further requirements.
6.1(d) Vital interests	No further requirements.
6.1(e) Public Interest	Not applicable. See response on pg. 2 above.
6.1(f) Legitimate Interest	No further requirements.

Comment: Elements (e) and (f) regarding data subject rights are part of our existing obligations under GDPR and likely don’t need to be specifically included in the policy.

Building block i) (Query Policy)

The EPDP Team recommends that the entity disclosing the data:

a) May take measures to limit the number of requests that are submitted by the same requestor if it is clear that the requests are not legitimate and of an abusive nature;

b) Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system, such as unjustified, high-volume automated queries;

c) [Other]

A response to an SSAD request must not include more non-public data elements than have been requested by the requestor. The response must include the public data elements related to the domain name registration.

An SSAD request meeting the requirements as outlined in these policy recommendations must be received for each domain name registration for which non-public registration is requested to be disclosed. Each such request should be examined on its own merits.

Please specify what additional requirements need to apply or do not apply if it concerns a disclosure request for which the controller discloses under the following lawful basis:

6.1(a) Consent	Generally not applicable given that practically speaking, where consent of the data subject has been obtained for publication of their personal data, that data should be available under a general public query of the data. Note, however, that unless we obtain consent for any and all use of data in the public domain, without limitation, use is only limited to the purpose for which the consent has been obtained. Even if the data is published, we must ensure there are appropriate safeguards to ensure that use of the data does not exceed the scope of consent.
6.1(b) performance of contract	No further requirements.
6.1(c) Legal obligation	Need more information to determine what legal requirements might supersede query policy based on the relevant legal obligation.
6.1(d) Vital interests	Need more information to determine what legal requirements might supersede query policy based on the relevant vital interest.
6.1(e) Public Interest	Not applicable. See response on pg. 2 above.
6.1(f) Legitimate Interest	No further requirements.

	Building block k) (Receipt of acknowledgement) The EPDP Team recommends that, consistent with the EPDP Phase 1 recommendations, the response time for acknowledging receipt of a SSAD request should be without undue delay, but not more than two (2) business days from receipt, unless shown circumstances does not make this possible. The response should also include information about the subsequent steps as well as the timeline consistent with the recommendations outlined below. *Please specify whether a different response time should apply if it concerns a disclosure request for which the controller discloses under the following lawful basis:*
6.1(a) Consent	Generally not applicable given that practically speaking, where consent of the data subject has been obtained for publication of their personal data, that data should be available under a general public query of the data. Note, however, that unless we obtain consent for any and all use of data in the public domain, without limitation, use is only limited to the purpose for which the consent has been obtained. Even if the data is published, we must ensure there are appropriate safeguards to ensure that use of the data does not exceed the scope of consent.
6.1(b) performance of contract	No requirement for different response time for acknowledgement.
6.1(c) Legal obligation	No requirement for different response time for acknowledgement.
6.1(d) Vital interests	Where the vital interest claimed suggests that an urgent response is required, a shorter time period for acknowledgement may be justified. This accelerated response time would only be available based on a real and demonstrable urgent need. Note that in most cases, an urgent request is more appropriately routed directly to the Contracted Party holding the data.
6.1(e) Public Interest	Not applicable. See response on pg. 2 above.
6.1(f) Legitimate Interest	No requirement for different response time for acknowledgement.

	Taking into account the following principle identified during the F2F meeting, namely full automation may not be possible, but automation should be the goal where possible, please identify the parts of the disclosure request for which it may NOT be possible to automate.
6.1(a) Consent	Disclosure on the basis of consent is fully automated since the data should appear in the publicly available RDS.
6.1(b) performance of contract	The determination of whether a contract exists which covers the disclosure of data under a specific request cannot be fully automated.

6.1(c) Legal obligation	The evaluation of whether an appropriate legal obligation exists which covers the disclosure of data under a specific request cannot be fully automated.
6.1(d) Vital interests	The evaluation of whether an appropriate vital interest exists which covers the disclosure of data under a specific request cannot be fully automated.
6.1(e) Public Interest	Not applicable. See response on pg. 2 above.
6.1(f) Legitimate Interest	The decision regarding whether a request satisfies the 6.1(f) balancing test cannot be automated.

	Please identify types / categories of requests for which responses could potentially be standardized
6.1(a) Consent	Disclosure on the basis of consent is fully automated since the data should appear in the publicly available RDS.
6.1(b) performance of contract	All inputs into the system have the potential for standardization.
6.1(c) Legal obligation	All inputs into the system have the potential for standardization.
6.1(d) Vital interests	All inputs into the system have the potential for standardization.
6.1(e) Public Interest	Not applicable. See response on pg. 2 above.
6.1(f) Legitimate Interest	All inputs into the system have the potential for standardization.