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.

GENERAL COMMENT FROM RrSG:
How can we use a GDPR legal basis for global policy and in our building blocks? What might be a legal basis under the GDPR might not be a basis under the CCPA.

The CCPA rivals the GDPR and sometimes goes beyond the GDPR. Due to the fact the CCPA is more detailed compared to the GDPR, it makes it impossible to apply a GDPR program globally and achieve compliance. The CCPA applies to consumers; while there is overlap with natural persons, it is a distinction. The CCPA's definition of personal information is more extensive and goes beyond the definition in the GDPR.

While it was practical to use the GDPR in our discussions, it cannot be the only legal basis for our work, but a more holistic approach is required to meet all the data protection requirements globally.

Currently emerging is the APEC CBPR. We most likely have a blindspot there (and other data protection laws) on the requirements for such business certifications.

[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	Not applicable. Note: Further clarity is required because there is more than one way to read the proposed language
6.1(b) performance of contract	Not applicable as it refers to the contract between the data subject and requestor.
6.1(c) Legal obligation	Exact reference to the regulations or laws giving rise to the legal obligation, specific information on how these apply in this case.
6.1(d) Vital interests	Details on the vital interests affected. Details how disclosure is necessary to protect those interests (e.g. no simpler means). details how disclosure will protect those vital interests.
6.1(e) Public Interest	Not applicable as controller neither has official authority nor is it performing tasks in public interest.
6.1(f) Legitimate Interest	Detailed explanation of legitimate interest in the disclosure, no mere reference of rights or issues, specific information required that it tailored to the specific request. For example in case of an alleged trademark violation, the request should include details on how the registration or its use constitutes an obvious violation of the trademark, not a mere reference to a trademark and claim of (potential) violation. Add reference materials, where possible.

	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	All not applicable, you set all your terms within the AUP itself. To satisfy GDPR requirements it would require an SCC as mentioned by the legal opinion of B&B.
6.1(b) performance of contract	Not applicable, see above
6.1(c) Legal obligation	Not applicable, see above
6.1(d) Vital interests	Not applicable, see above
6.1(e) Public Interest	Not applicable, see above
6.1(f) Legitimate Interest	Not applicable, see 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	Not applicable. Note: Further clarity is required because there is more than one way to read the proposed language
6.1(b) performance of contract	Unclear how performance of a contact would be applicable here as the disclosing party still maintains the ability to review each request and can not be contractually obligated to disclose such data on a mandatory basis.
6.1(c) Legal obligation	Unclear what specific legal obligation (absent a court order from applicable jurisdiction) could apply in this case.
6.1(d) Vital interests	Demonstration from the requester of the specific vital interest in question...and to be clear, the vital interest in 6.1(d) is to protect the data subject as opposed to the vital interest of the requester.
6.1(e) Public Interest	Unclear how that could apply in this case.
6.1(f) Legitimate Interest	Presumably, the disclosing party has done a balancing test and determined the data subjects' right outweigh the legitimate interest cited in the disclosure request so the requesting party would need to amend and provide additional information which could be used in further review of the request.

Building block h) (Acceptable Use Policy) (Discloser)

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	No further requirements
6.1(f) Legitimate Interest	No further requirements

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	Not applicable. Note: if the Disclosing Entity has obtained consent, data should be publicly available. Consent is either "universal" or withheld, we cannot operationally manage a per-requestor consent framework on behalf of data subjects.
6.1(b) performance of contract	Request should include some indication of the contract between Requestor and Data Subject (e.g. activation of a product requiring DNS).
6.1(c) Legal obligation	Unknown
6.1(d) Vital interests	Unknown. Do we want to allow LEA to have the ability to submit multiple domain names if they affirm these are part of the same investigation? Or does this open the door to Civilian/IP abuse?
6.1(e) Public Interest	Unknown
6.1(f) Legitimate Interest	Unknown

	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	There is no requirement for a different response time here. Note that this would be the data subject (domain owner) consenting, not the requestor.
6.1(b) performance of contract	There is no requirement for a different response time here.
6.1(c) Legal obligation	There is no requirement for a different response time here. B&B Legal memo on this lawful basis doesn't speak to response time.
6.1(d) Vital interests	In cases where the requestor can demonstrate that someone's life is at risk, an immediate response time may be warranted. If these requests go through the SSAD there would need to be a structure to indicate the urgent nature of the issue, which complicates SSAD operations. The requestor may instead go directly to the controller, eliminating the need for the SSAD to accommodate this type of circumstance.
6.1(e) Public Interest	There is no requirement for a different response time here.
6.1(f) Legitimate Interest	There is no requirement for a different response time here.

	*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	Consent cannot be granted in an automated manner. Requesting consent and tracking/logging the response could be automated.
6.1(b) performance of contract	It is not possible to automate the determination of whether there is a contract in place which covers the disclosure of data.
6.1(c) Legal obligation	It is not possible to automate the determination of whether there is a legal obligation at hand which covers the disclosure of data.
6.1(d) Vital interests	It is not possible to automate the determination of whether there is a vital interest at hand which covers the disclosure of data.
6.1(e) Public Interest	It is not possible to automate the determination of whether there is a public interest at hand which covers the disclosure of data.
6.1(f) Legitimate Interest	It is not possible to automate the balancing test required when this is the lawful basis for disclosure.

	Please identify types / categories of requests for which responses could potentially be standardized
6.1(a) Consent	All response formats can be standardized. This doesn't mean that responses always include the same info (it could be a subset of the possible options)
6.1(b) performance of contract	See above
6.1(c) Legal obligation	See above
6.1(d) Vital interests	See above
6.1(e) Public Interest	See above
6.1(f) Legitimate Interest	See above