Step 1: Preliminary Assessment of the request – 6(1)f

a) **Who is the requester?**

If this identity or the 'trustworthyness' is not clear - needs to be verified.

A subset of our policy work should be focussed on the means to make such identification of the requesters easier for all concerned - i.e. **Accreditation (**note accreditation at its most basic relates to identity only and not the validity of an individual request)

b) **For what reason [as stated, not assumed] is the data needed?**

Necessity is not absolute; however, it must be reasonable *in the specific circumstances*. If the reason is not made out sufficient in the specific circumstances, then this must be queried with the requester.

c) **Is the release of the data necessary to achieve the purpose, as stated?**

i.e. are there any less invasive means, reasonably available to the requester, to achieve the desired result/outcome? e.g. a consumer wishes to purchase a domain name and requests release of registrant data. This is a reasonable request; however, under the temp spec a registrar will relay any such message to the registrant, without need for disclosure of the email. Therefore, this release of the data is not reasonably necessary - UNLESS the requester can confirm they have tried to contact the registrant via this means, and such an option was not available at the registrar: NOTE: if the option was available, and a registrant chooses not to respond to such a communication, then this does not change the necessity, nor can we as controller assume otherwise - i.e. no response does not establish additional necessity in this instance.

d) **What data is being requested? Are the data elements requested limited and reasonable to achieve the purpose as stated?** The release of each data element must be assessed individually. If a request is over-broad, it may taint the entire request, as it affects the bone fides of the request, and tends to suggest insufficient consideration as to necessity and reasonableness is grounding the request; this means that the effect on the rights of the data subject is not core in the consideration. Again, in the above example [although a minor example] if I want to buy a domain name, my request should be limited only to the email address in the 1st instance (or my preferred method of communication - however the email is the least invasive and necessity would likely dictate that unless justified, the email address is the only data required). I really don't need the name of the registrant to make my offer. Any request that merely asks for all registrant data, raises the bar of necessity, and the requester who does not exercise due care in the request, will find that count against them in the balance.

Step 2: Assessment of the data being requested

Once the validity of the request has been established, **only then** should the actual data be processed by the controller (as in truth, until a valid, prima facie case for disclosure has been received the actual CONTROLLER does not have a sufficiently valid reason, as controller, to process the data to consider disclosure). You may call this overcautious - but this is Privacy by Default and Design in action.

a) **Does the data requested contain personal data?**

This is an ‘eyes on’ review as Skynet has not yet been launched and the DNS has not been built with such inbuilt consideration. If there is no PII in the data requested, then release is likely possible. (Brian King, on the thread you noted, again, the Legal v Natural issue, this is of course a part of the consideration of the controller - just because we don't have the technological safeguards to be able to securely differentiate for publication, that does not mean that we won't release this data once assessed as not containing PII.)

b) **If it contains Personal Data, does the data originate from within the EEA? [additional requirements may be necessary here - this is up to the individual controller to identify and apply any local requirements also e.g. for US companies (or non-us companies as the case may be), does processing fall under CCPA)**

- If satisfied that the data is non EEA (or is not subject to another relevant requirement peculiar to that controller), then the data may be released.
- If the data is PII and from within the EEA, then the balancing test must occur…

Step 3: Apply the Balancing Test: (paraphrased from the Bird & Bird advices received during EPDP Phase I – based on *Rigas*)

1) *Assessment of impact.* The controller must consider not only adverse outcomes on individuals, but also other broader consequences for data subjects: "*Relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of the data processing*".

2) *Nature of the data.* This factor requires consideration of the level of sensitivity of the data as well as whether the data is already publicly available.

3) *The way the data is processed.* The manner in which the data will be processed affects the balance of interests. Of particular relevance, the WP29 states, "*whether the data are publicly disclosed or otherwise made accessible to a large number of persons*" is an important consideration if "*[s]eemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data*".

4) *The reasonable expectations of the data subject.* Whether an individual is likely to expect the processing activity will affect the balance of interests. This concept also appears in Recital 47 of the GDPR, which states, "*the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place*".

5) *The status of the controller and data subject.* Finally, the assessment must take into consideration the negotiating power and any imbalances in authority between the controller and the data subject. Thus, this analysis changes depending on both the status and authority of the controller and the relative power of the data subject.

RESULT:

1) Based on the **documented** conclusions (individual and specific to that request) of all 3 Steps you feel the request is justified – **release is permitted**.

2) If you feel that the balance is not favouring release – Respond to requester noting that the data **shall not be released** and **provide a reason for such a conclusion**.

3) The requester may of course re-request, and remedy those issues raised.

   Note: for subsequent requests relating to the same data, the controller must assess incompatibilities between different iterations of the request, as any exercise in 'ticking boxes' as opposed to genuine efforts to respect the rights of the data subject, and the responsibilities of the controller should be part of subsequent balancing tests (and, where applicable may go towards raising issues with accreditation etc.)