Feasibility of unique contacts – Input Received (Status 12 January 2021)

Definitions (derived from the legal committee questions):

Unique contacts: the option of replacing the email address provided by the data subject with an alternate email address that would in and of itself not identify the data subject.
Pseudonymisation: the same unique string is used for multiple registrations by the data subject.
Anonymization: the string would be unique for each registration by the data subject.

Clarifying questions in relation to legal memo (see https://community.icann.org/x/YoAmCQ)

Definitions

1. Clear, universally accepted definitions:
   a. Uniform: over what scope?
   b. Pseudonymisation: over all registrations, or within a registrar?
   (Alan Greenberg & Hadia El Miniawi, ALAC)

2. To supplement the comment above regarding the need to achieve a common understanding on the various terms used:
   What is unique *vs* uniform contact? In the legal memo it is mentioned that:
   "where the same unique string would be used for multiple registrations by the data subject" → this would be 'pseudonymisation', and "where the string would be *unique for each registration*" → this would be 'anonymization'. At some point, there was reference to 'uniform' contact as a contact which remains the same across all registries/registrars. Does this mean that the unique string remains or not? (Melina Stroungi, GAC – p.1)

Relevance of CP retaining personal data

Paragraph 8: Regardless of whether or not the data would be considered personal data from the third party's perspective, it can still be personal data at least from Contracted Parties/ICANN's perspective and (for some data protection authorities) this also affects whether it is personal in the hands of the recipient – as set out in the position taken by the Article 29 Working Party's 2014 Opinion on Anonymization techniques [ec.europa.eu], also mentioned at the outset of this advice:"when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data."

3. Relevance of ¶ 8 -- why is fact that CP's retain personal data relevant? They have Registrant personal data by virtue of their business relationship, hence they do not have additional PI by virtue of anonymizing. (Laureen Kapin, GAC – page 2-3, paragraph 8)

Masking

"We think either option ((a) or (b)) would still be treated as the publication of personal data on the web. This would seem to be a case covered by a statement made in the Article 29 Working Party's 2014 Opinion on Anonymization techniques [ec.europa.eu]: *"when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data."*

4. What is the relevance of introducing the concept of "masking" (ie blocking part or parts of the original address) when that concept was never suggesting in respect to email addresses? (Alan Greenberg & Hadia El Miniawi, ALAC)

Pseudonymisation

5. Could we have an example of how 'pseudonymisation' would work in practice?
   The legal memo defines pseudonymisation as 'the same unique string being used for multiple registrations by the data subject'. However it does not further explain:
   1) how a unique string can be used for multiple registrations (e.g., do the different registrars communicate at the time of registration and exchange this unique string along with other personal data of the registrant? Or is there a common database where all strings corresponding to each registration are listed?)
   2) how different information of the individual can be combined to trace back to that individual (which is the GDPR definition of pseudonymisation).
   Assuming that different information can be combined to trace back to that individual, would such tracing be possible only for registries/registrars or also for third parties? (Melina Stroungi, GAC – p.1)

General/Conclusions

6. Hasn't the legal memo already established that a pseudonymized email is personally identifiable information and should not be published? (Milton Mueller, NCSG – Summary, page 1)
7. Isn't key issue re: publication of anonymized email whether the email is anonymized with respect to 3rd parties (i.e. other than the data controller(s))? (Laureen Kapin, GAC)
8. For anonymized data (ie 1 string per registration), the question is not whether it is personal data but to assess the potential harm to the data subject or what the risk is to the registrar to publishing it. GDPR does not prohibit publication of personal data but does require that there be sufficient off-setting benefit - the balancing test as per GDPR 6(1)(f). (Alan Greenberg & Hadia El Miniawi, ALAC)
9. The memo declares that pseudonymized data "could be personal data" (and specifically mentions Breyer, which provides clarity regarding when it would not be considered personal data by a third party); while it's clear that the pseudonyms are always considered personal data by the contracted party, it's not always the case for those 3rd parties whose

processing does not result in reconstruction of the original contact data. More analysis should be performed regarding the use of pseudonyms by those 3rd party use cases. (Margie Milam & Mark Svancarek, BC – page 3, 5, 7, 8)

10. The Legal memo concentrates on the use of the email as a means by which to contact the registrant. If the primary use for a pseudonymised email is for statistical or research reasons does this affect the link to the data subject and effect on them with regards to the function of processing the data. (Chris Lewis-Evans, GAC)

Experience

11. To what extent have registrars relied on changing anonymized addresses over time, and what periodicity? (Alan Greenberg & Hadia El Miniawi, ALAC) (Alan Greenberg & Hadia El Miniawi, ALAC)

General statements

12. The summary seems to make certain assumptions about use case and implementation (specifically that contacting a registrant using their pseudonym is intended to identify them, or that the act of using a pseudonym will identify them regardless of intent) which are not necessarily true. The longer analysis portion is more useful for our work. (Margie Milam & Mark Svancarek, BC)

Proposals: What options to require unique contacts to have a uniform anonymized email address across domain name registrations would not result in being treated as publication of personal data.

1. Requirement to have a functional email address is necessary (whether pseudonymized, anonymized, seen or unseen, etc.); web form has proven not to be a workable option. (Brian King, IPC)
2. Investigate whether it is possible, once a person's email address is anonymised towards third parties but effectively pseudonymised towards Registries/Registrars, to identify that person in any way, other than by utilising confidential information the registry/registrar itself has or a leak of information from the registry/registrar. If there is no other way to identify the person then there is no additional risk in anonymizing as the Registry/Registrar would anyway have this personal information and the risk of leaking would remain irrespective of publishing the (pseudo)anonymized email. (Melina Stroungi, Chris Lewis-Evans (GAC) – page 2, paragraph 8 of legal memo)