



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

DNS4EU

Background



- In late 2020, the European Commission published a Joint Communication (with the High Representative of the Union for Foreign Affairs and Security Policy), 'The EU's Cybersecurity Strategy for the Digital Decade'
 - Under Section 1.6 *Greater global Internet security*:

With a view to reducing security issues related to market concentration, the Commission will encourage relevant stakeholders including EU companies, Internet Service Providers and browser vendors to adopt a DNS resolution diversification strategy. The Commission also intends to contribute to secure Internet connectivity by supporting the development of a public **European DNS resolver service**. This 'DNS4EU' initiative will offer an alternative, European service for accessing the global Internet. DNS4EU will be transparent, conform to the latest security, data protection and privacy by design and by default standards and rules and form part of the European Industrial Alliance for Data and Cloud⁶³.

Current activity



- On 12 January 2022, as part of the Connecting Europe Facility (CEF) programme, the Commission launched a tender:
 - *‘Equipping backbone networks with high-performance and secure DNS resolution infrastructures - Works’*



Objectives



- *“The deployment of DNS4EU aims to address such consolidation of DNS resolution in the hands of few companies, which renders the resolution process itself vulnerable in case of significant events affecting one major provider.”*
- *“Moreover the lack of significant EU investment in the field hampers the development of infrastructures that favour the detection and filtering of local cyber-threats that nonetheless could have significant socio-economic impacts.”*
- *“In addition, the processing of DNS data can have an impact on privacy and data protection rights.”*

More specifically...



- *“...shall offer a high level of resilience, global and EU-specific cybersecurity protection, data protection and privacy according to EU rules”*
- *“...ensure that DNS resolution data are processed in Europe and personal data are not monetised”*
- *“...shall adhere to the latest internet security and privacy standards”*
- *“...shall be widely discoverable and easy to configure by end-users on their equipment and software”*
- *“...shall offer additional optional services such as free parental control, as well as paid premium services for enhanced performance or security for corporate users”*

Additionally...



- *The proposal for the service infrastructure shall comply with EU regulation and applicable national regulations of its Member States, in particular:*
 11. *Data protection and privacy: Compliant with GDPR and national rules, where applicable.*
 12. *Lawful filtering: Filtering of URLs leading to illegal content based on legal requirements applicable in the EU or in national jurisdictions (e.g. based on court orders), in full compliance with EU rules.*
- *Priority will be given to proposals addressing the following aspects:*
 14. *Governance/Federated structure: A federated and expandable service infrastructure with a diverse membership is preferred in order to maximise the footprint and customer base of DNS4EU across the EU, reduce costs through shared resources and ensure the long-term sustainability of DNS4EU.*

Key details



- Grants of up to 14m EUR, for costs
 - “...related to the development, construction and deployment”
 - “Costs for operating the infrastructure during its lifetime will be excluded under the call.”

Timetable and deadlines (indicative)	
Call opening:	12 January 2022
<u>Deadline for submission:</u>	<u>22 March 2022 – 17:00:00 CET (Brussels)</u>
Evaluation:	April-July 2022
Information on evaluation results:	August 2022
GA signature:	November/December 2022

...applicants (beneficiaries and affiliated entities) must:

- be legal entities (public or private bodies)
- be established in one of the eligible countries, i.e. EU Member States (including overseas countries and territories (OCTs))

Questions for the community



- Is this project useful? Necessary?
- Do you have an interest in who ultimately takes on this project?
- Will this have any impact on current DNS operations in Europe? (...or beyond)?
- Are the requirements appropriate, realistic, comprehensive?
- Are there risks inherent in such an effort (for the users, operators, the DNS itself)?
- Does the RIPE community or RIPE NCC membership see any role for the RIPE NCC?

RIPE Community Feedback



- Concerns about possible obligations or requirements on network operators
- Represents a new kind and degree of government intervention
- Technical concerns re. centralisation or consolidation of DNS resolution services (a potential “single point of failure”)
 - A “federated” model may mitigate this concern
- Strong community interest in who is awarded the tender
 - No strong desire for the RIPE NCC to take an active role

<https://labs.ripe.net/author/chrisb/dns4eu-ripe-ncc-open-house-discussion>



Questions



chrisb@ripe.net
@_buckr