# European DNS Resolver Policy

4th September 2020

## Introduction

The European DNS Resolver policy sets out the minimum policy and transparency requirements that need to be adhered to by operators of compliant DNS resolver services. It is intended to provide reassurance to stakeholders that data gained in the operation of DNS resolution services are not used for any other purposes except where required by law or regulation or with the explicit informed consent of the end user.

In addition, the policy offers some advice to operators of DNS resolution services on the provision of optional filtering capabilities that customers can choose to use (or not) for purposes such as malicious content protection and parental controls. The policy also provides some guidance on how these features could be offered to customers.

These DNS resolution services can support a range of DNS transports including, but not necessarily limited to, any combination of Do53, DoT, DoH and DoQ.

It is hoped that companies responsible for software that interacts with the DNS, particularly operating systems and web browsers, will prefer to specify DNS resolution services that comply with this policy.

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT" and "MAY" in this document are to be interpreted as described in RFC 2119 as published by the Internet Engineering Task Force[1].

## Privacy Requirements

Operators of DNS resolver services SHOULD make technology and operational choices that protect user privacy. These services SHOULD be operated in a manner that matches or exceeds the protections described in all relevant EU Directives and Regulations. These include but are not necessarily limited to GDPR[2] and ePrivacy[3]. Compliance with prevailing legislation[4] will also apply[5] — for instance, the enactment of EU Directives in national or local law.

Except where required by law or with the explicit informed consent of the end user[6], operators of DNS resolver services:

i. MUST make, document and publish their operational practices to protect the privacy and security of their users' data.

ii. MUST publish their transparency and privacy policy so that it is publicly available.

iii. SHOULD support relevant Internet standards to protect or enhance privacy and validate DNS responses.

iv. SHOULD operate their service in a fair, non-discriminatory manner.

v. SHOULD NOT retain or transfer to any third party any data arising from the use of these services[7] except where anonymised data is necessary for cybersecurity, DNS analytics, reporting and research purposes[8].

vi. SHOULD NOT directly or indirectly monetise[9] any data[7] arising from the use of these services and SHOULD NOT enable other parties to monetise[9] the data either.

vii. SHOULD NOT use or require HTTP cookies when communicating with DNS clients that use HTTP-based DNS transports for resolution.

viii. SHOULD ensure session length and ticketing parameters for TLS-based DNS transports follow industry best practices for the optimal privacy outcomes.

ix. MAY direct the user to alternative content in order to protect them from exposure to inappropriate content[10]. Any such circumstances need to be clearly documented within the transparency and privacy notice.

x. MUST update their policies and practices in a timely manner when notified of any unintentional breaches of the above points, for example when new user identifiers become known.

## Security and Filtering Requirements

Operators of DNS resolver services:

i. MUST comply with legal or regulatory requirements and SHOULD comply with industry best practices to block access to unlawful content. If such blocking is required, information on the categories of such material MUST be provided in the transparency and privacy notice unless explicitly prohibited by law. Accurate and complete details of either (a) any domains that are actively blocked or (b) threat feeds used to block such domains MUST be accessible to a user unless explicitly prohibited by law. In addition, any blocking events or activities that are not domain-based MUST be clearly documented in the transparency and privacy notice or another publicly accessible portion of the resolver operator's website unless explicitly prohibited by law.

ii. MAY support optional DNS filtering capabilities, which could include but are not limited to parental controls and malicious content protection[11]. Where customisation options are offered to individual users, the DNS resolver operator SHOULD ensure that this does not facilitate disclosure of Personal Data, identification of end users, or behaviour beyond that needed by the resolver service to identify the client for filtering purposes. Any filtering options and details of how to opt in/out of using these SHOULD be clearly explained in the transparency and privacy notice.

iii. The resolver operator SHOULD share anonymised cyber intelligence information with appropriate stakeholders which may include national and regional Computer Security Incident Response Teams, cyber security agencies, law enforcement agencies, research institutions and other authenticated, benign third-party cybersecurity actors.

## Transparency Requirements

The DNS resolver operator MUST have a publicly available transparency and privacy notice. This notice MUST use plain language that a typical user could reasonably be expected to understand and MUST cover the following:

i. The national jurisdiction that it operates under.

ii. Confirmation that all activities and practices, including those covered in this section, comply with relevant EU Directives and Regulations as well as relevant national and local legislation and regulations.

iii. An explanation of the nature of any Personal Data that is collected or processed during operation of the service.

iv. A summary of which categories of data, if any, are retained by the operator[12], for what period of time, with a clear indication of which categories of data are anonymised and what Personal Data, if any, is stored or processed. Any Personal Data SHOULD be minimised and the transparency and privacy notice MUST clearly state why each type of data is retained, e.g. for research purposes.

v. A summary of any categories of anonymised data that are shared with third parties and why, e.g. for cybersecurity, DNS analytics, reporting or research purposes.

vi. A description of the general categories of unlawful content that can be blocked, citing the relevant legislation or regulation. As noted in the Security and Filtering Requirements section, information on the categories of such material MUST be provided unless explicitly prohibited by law. Accurate and complete details of either (a) any domains that are actively blocked or (b) threat feeds used to block such domains MUST be accessible to a user unless explicitly prohibited by law[13]. In addition, any blocking events or activities that are not domain-based MUST be clearly documented, either in the transparency and privacy notice or another publicly accessible portion of the resolver operator's website, unless explicitly prohibited by law. The transparency and privacy notice SHOULD NOT disclose information that would be helpful to those seeking to access the blocked content[14].

vii. An outline of any filtering options that are provided and details of how to opt in/out of using these facilities. This information SHOULD NOT disclose information that would be helpful to those seeking to bypass or reverse engineer these filters.

viii. Details of a complaints procedure to handle false positives and false negatives generated by any filtering or content blocking capabilities that are available.

ix. A description of the circumstances where an operator of a DNS resolver service MAY direct the user to alternative content and the nature of that content— for example to an explanatory web page whenever malicious content protection has been enabled and an attempt was made to look up a blocked domain name.

x. An explanation of who is permitted to use the DNS resolver service whenever it is not provided to the general public — for example by an ISP that restricts the service to those connected to the ISP's network.

xi. Details of any other relevant operational practices that protect privacy.

## Notes, Definitions and References

1. See https://tools.ietf.org/html/rfc2119

2. The EU General Data Protection Regulation – see https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

3. The EU Directive on privacy and electronic communications – see https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive

4. The resolver operator must state in its transparency and privacy notice the relevant national jurisdiction that it operates under

5. For example: if Spain were the national jurisdiction stated in the transparency and privacy notice this would include the Data Protection and Digital Rights Law (Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales); if it were the UK, this would include the Data Protection Act, Digital Economy Act and Information Commissioner's Office Data Anonymisation Code of Practice.

6. For resolver operators that neither directly interact with end-users nor access or process Personal Data, it will not be possible to gain informed consent from end-users as they do not interact with such services. In these instances, the resolver operator needs to ensure that any variation from the practices described in the Privacy Requirements section is documented in their Transparency and Privacy Policy and that this is readily accessible.

7. This includes but is not limited to: Personal Data; IP addresses or other user or device identifiers; user query patterns consistently associated with a natural person or specific device from the DNS queries sent from the client; cache miss data.

8. This has to be done using anonymisation techniques that are consistent with the relevant rules and standards that protect users' personal data and privacy. See for example the Data Anonymisation Code of Practice from the UK Information Commissioner's Office.

9. Leverage for commercial or operational gain in any way. This includes but is not limited to: the sale of the data; machine learning based on it or associated anonymised data; leveraging the resolver operation in IPX peering deals; leveraging the resolver operation in the sale of CDN services to provide optimised performance to clients; other quid pro quo arrangements.

10. For example, an explanatory splash page if malware protection is enabled and a user tries to access a blocked domain name.

11. Sites or content which have criminal intent by the content operator towards the client by delivering a result that is unexpected by the client, such as malware, phishing, spyware, counterfeit information, or other deceptive or harmful results.

12. Noting that DNS resolvers may have to comply with relevant laws or regulations applying to data retention (i.e. minimum or maximum retention time etc. as provided in the GDPR and in other relevant rules).

13. Unless prohibited by law or regulation, blocking information should be available for a period of twelve months from the point that it becomes applicable or until the block is no longer active, whichever is the longer.

14. To avoid aiding the bypassing or reverse engineering filters, resolver operators MAY limit their disclosure to, for example, URLs or blocklists.