European DNS Resolver Policy

13th May 2021

Introduction

The European DNS Resolver policy sets out the minimum policy and transparency requirements that should be adhered to by operators of Domain Name System (DNS) resolver services. It is intended to provide reassurance to end-users and other stakeholders that personal data[1] gained in the operation of DNS resolution services are not used for any other purposes except where required by law or regulation, or with GDPR-level consent of the end-user and where it is clearly documented in the operator's transparency and privacy statement.

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 capitalised words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT" and "MAY" in this document are to be interpreted as described in RFCs 2119 and 8174 as published by the IETF (Internet Engineering Task Force)[2].

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 privacy and related protections described in all relevant EU Directives and Regulations. These include but are not necessarily limited to GDPR[3] and ePrivacy[4]. Compliance with prevailing legislation[5] will also apply — for instance, the enactment of EU Directives in national or local law[6]. Any user consent confirmations and information privacy practices should be at least consistent with those requirements specified in GDPR and national law.

Except where required or prohibited by law or with GDPR-level consent of the end user[7,8], operators of DNS resolver services:

i. MUST make, document and publish their operational practices to protect the privacy and security of their users' data. The practices documented in section 5 of the IETF's RFC 8932[9] ("Recommendations for DNS Privacy Service Operators") SHOULD be adopted for this reason.

ii. MUST publish their transparency and privacy policy so that it is publicly available and easily accessible at any time, including as part of a subject access request.

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

iv. SHOULD NOT retain or transfer to any third party[10] any personal data arising from the use of these services except where anonymised[11] or aggregated[12] data is necessary for cybersecurity, DNS analytics, reporting and research purposes. NB If it is possible to use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised (ie it is still effectively personal data and should be treated as such).

v. SHOULD NOT directly or indirectly monetise[13] any personal data arising from the use of these services and SHOULD NOT enable other parties to monetise the data either. NB Where any other data is to be monetised by either the resolver operator or a third party, care MUST be taken to ensure that it is not possible to use any reasonably available means to re-identify the individuals to which the data refers, otherwise that data will not have been effectively anonymised but will have merely been pseudonymised (ie it is still effectively personal data and should be treated as such).

vi. SHOULD NOT use or require HTTP cookies or other tracking techniques when communicating with DNS clients that use HTTP-based DNS transports for resolution.

vii. SHOULD ensure session length and ticketing parameters for TLS-based DNS transports follow industry best practice designed to improve user privacy, for example by ensuring that session lengths are kept to the minimum length possible rather than being extended for better performance.

viii. SHOULD offer support for one or more encrypted DNS transports where these are defined in international standards by a recognised body such as the IETF.

ix. MAY direct the user to alternative content in order to protect them from exposure to inappropriate or unwanted content[14]. Any such circumstances need to be clearly documented within the transparency and privacy notice.

x. MUST update their policies and practices promptly when notified of any unintentional breaches of the above points, for example when new user identifiers become known. In such circumstances, the transparency and privacy notice should be updated to indicate what breach was identified and what action was taken, together with any recommendations for others to follow.

Security and Filtering Requirements

The operators of DNS resolver services:

i. MUST comply with legal or regulatory requirements, including any requirements of the national jurisdiction stated in the transparency and privacy notice. If such blocking is required, information on the categories of blocked material MUST be provided in the transparency and privacy notice unless explicitly prohibited by law. Unless explicitly prohibited by law, where any domains are actively blocked, accurate and complete information MUST be accessible that detail the categories of content covered by any threat feeds or similar mechanisms. 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. Resolver operators MAY respond to non-automated requests for clarification of the reason for access to content being blocked with an indication of the reason for that block.

ii. MAY support optional DNS filtering capabilities, which could include but are not limited to parental controls and malicious content protection[15]. Care should be taken in offering DNS resolution without malicious content protection or the blocking of child sexual abuse material as a default option to non-expert end-users such as consumers unless it is unlawful to provide such protections. 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 the details of how to opt in and opt out of using them SHOULD be clearly explained in the transparency and privacy notice, together with the possible consequences of changing the options[8].

iii. In addition to any legal requirements to share cyber intelligence, the resolver operator SHOULD share 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. Where cyber intelligence information is shared, it MUST first be anonymised[11] or aggregated[12].and the receiving parties MUST be documented in the transparency and privacy notice unless it is unlawful to do so.

Transparency Requirements

The DNS resolver operator MUST have a publicly available transparency and privacy notice[16] that is readily accessible. This notice MUST use plain language that a typical user could reasonably be expected to understand and MUST cover the following:

i. The name of the legal entity responsible for the operation of the resolver, together with its trading name if different and confirmation of the national jurisdiction[5] that it operates under, noting any overarching legal requirements on blocking, data access and data retention together with details of any other aspects of the operation of the resolver that may affect user privacy.

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 based on the national jurisdiction stated in the transparency and privacy notice.

iii. An explanation of the nature of any Personal Data that is collected or processed during operation of the service and clarification why it is necessary to do so.

iv. A summary of which categories of data, if any, are retained by the operator[17], 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, for what purpose and what parties will have access to it.

v. Unless explicitly prohibited by law, details of the number of requests received for resolver data from law enforcement agencies and resulting from other legal processes, together with details of the number of new blocking requests received from law enforcement agencies and other legal processes. Such details should include the origin of the request(s) and whether subsequent action was taken by the operator resolver.

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

vii. A description of the general categories of unlawful content that can be blocked, citing the relevant legislation or regulation(s). As noted in the Security and Filtering Requirements section, information on the categories of such material MUST be provided unless explicitly prohibited by law. Unless explicitly prohibited by law, where any domains are actively blocked, accurate and complete information MUST be accessible that detail the categories of content covered by any threat feeds or similar mechanisms[18]. 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[19].

viii. 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.

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

x. 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.

xi. 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.

xii. Details of any other relevant operational practices that protect privacy, including any additional requirements covered by legislation or regulation.

Notes, Definitions and References

1. Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2. See https://www.rfc-editor.org/rfc/pdfrfc/rfc2119.txt.pdf and https://www.rfc-editor.org/rfc/pdfrfc/rfc8174.txt.pdf

3. The EU General Data Protection Regulation – see https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. From January 2021 this is superseded by the UK GDPR in the UK.

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

5. *The resolver operator MUST state in its transparency and privacy notice*

    a. *Either the relevant national jurisdiction in which it operates. NB A resolver operator providing distinct services in multiple jurisdictions (eg an ISP with networks in multiple countries, each with its own, closed resolver) MUST provide a separate declaration for each jurisdiction in which it operates.*

    b. *Or, for a resolver operator providing the same service across multiple jurisdictions (eg a cloud-based resolver operator), a declaration of the jurisdiction(s) in which it operates.*

    Whether or not the resolver operator indicates that one or more jurisdictions apply, it must also detail all of the privacy and related protections, directives, legislation and regulations with which it complies.

6. 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 2018, Digital Economy Act and Information Commissioner's Office Data Anonymisation Code of Practice.

7. For resolver operators that neither directly interact with end-users nor access or process Personal Data, it will not be possible to gain GDPR-level 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.

8. Outside of the consumer environment, users wishes and requirements may be those expressed by an organisation rather than every individual user within it. For example, an enterprise may specify the options and policies to be applied to its employees, as may an educational establishment on behalf of its students. In the consumer environment, choices may be made by an account holder on behalf of other members of a household – this can often be the case for ISP-supplied services.

9. See https://www.rfc-editor.org/rfc/rfc8932.pdf.

10. Third party: Any legal entity other than that named in the transparency and privacy notice as being responsible for the operation of the resolver.

11. Anonymised data: data that does not relate to an identified or identifiable natural person or to personal data rendered anonymous using non-reversible techniques in such a manner that the data subject is not or is no longer identifiable*. NB If it is possible to use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised (ie it is still effectively personal data and should be treated as such). *See for example the Data Anonymisation Code of Practice from the UK Information Commissioner's Office (https://ico.org.uk/media/1061/anonymisation-code.pdf).

12. Aggregated data: numerical or non-numerical information that is collected from multiple sources and/or on multiple measures, variables, or individuals and compiled into data summaries or summary reports, typically for the purposes of public reporting or statistical analysis. It may include data that is derived from personal data but is not considered personal data if the aggregated data does not directly or indirectly reveal identities.

13. Leverage for commercial or operational gain in any way.

14. For example, an explanatory splash page if malware protection is enabled and a user tries to access a blocked domain name. Any such redirection should not be used as a means to monetise user activity by linking out to, or referencing, third parties.

15. 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.

16. References to a transparency and privacy notice in this document could be satisfied by a single document with that title or a variant of it, or with the necessary content split between separate transparency and privacy reports. Alternately, the necessary content could be incorporated within an extended version of an existing document or documents. An organisation will be deemed to meet this requirement if all of the specified content is available in a clearly labelled and readily accessible form that is easy to locate.

17. 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 legislation or regulations).

18. 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 longer.

19. To avoid aiding the bypassing or reverse-engineering filters, resolver operators MAY limit their disclosure to, for example, URLs or threat feeds.