Co-funded by
the European Union

DNS4EU Public Resolvers Policy

This is version of the Policy issued on 01.06.2025

Introduction

DNS4EU is an initiative by the European Commission. The Project is led by a Consortium of Partners with Whalebone as the Coordinator and CZ.NIC, Czech Technical University (ČVUT), Time.lex, deSEC, SZTAKI, Abi Lab, NASK and DNSC as other Project Partners.

The entity responsible for the operation of the DNS4EU Public Resolvers is Whalebone, s.r.o. company established and operating under the laws of the Czech Republic, ID No.: 05120403 registered in the commercial register kept by Regional Court in Brno, file C 93547 with registered seat at: Jezuitská 14/13, Brno 60200, Czech Republic.

This DNS4EU Public Resolver Policy sets out the policies regarding the privacy, data processing, filtering and transparency that the Consortium Partners adhere to (the "**Policy**"). Whalebone is the provider of 14 recursive DNS resolvers operated in 14 EU member states.

This Policy is based on Example RSP policy published by *the Internet Engineering Task Force* and incorporates the **DNS Resolver Recommendations** published by RIPE (Document ID: ripe-823).

DNS4EU Public Resolver

The DNS4EU Public Resolvers are recursive DNS resolvers that serve socio-economic drivers, public, corporate and residential internet end-users in the EU, and offer very high reliability and protection against cybersecurity threats, including those specific to the EU (e.g. phishing in EU languages).

DNS4EU Public Resolver infrastructure offers a high level of resilience, data protection and privacy according to EU Laws as well as national legislation, ensures that DNS resolution data is processed in the EU, and avoids collection of Personal Data to the greatest extent possible. It adheres to the latest internet security and privacy standards. It is widely discoverable and easy to configure by Users on their equipment and software.

A Guide on how to set up the DNS4EU Public Resolver can be found here (https://www.joindns4.eu/dns-guidelines) .

The DNS4EU Public Resolver infrastructure offers a scalable DNS resolution service comprising (i) the plain DNS resolution service without any restriction, filtering or content blocking and (ii) DNS resolution service with the following additional optional flavors configurable by the User:

- Protective DNS resolution
  - DNS4EU security layer
- Protective DNS with child protection filtering

Project number: 101095329 21-EU-DIG-EU-DNS, Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union

- Filtered content types are: Gambling, Sexual content, Weapons, Child abuse, Drugs, Racism, Terrorism and Violence

- Protective DNS with advertisement filtering
  - Filtered content type is Advertisement
- Protective DNS with child and advertisement filtering
  - Filtered content types are: Gambling, Sexual content, Weapons, Child abuse, Drugs, Racism, Terrorism, Violence and Advertisement
- Plain DNS resolution

DNS4EU Public Resolvers locations

All DNS4EU Public Resolvers are hosted within the datacenters controlled and operated within the EU as shown here. (https://www.joindns4.eu/for-public)

Definitions

Where the Conditions use the terms not defined hereunder, but defined in the Regulation (EU) 2016/679 (GDPR) respectively, those terms shall have the same meaning as in that Regulation (e.g. personal data, processing, etc.)

Aggregated data	refers to the collection and summarization of DNS query information across a large number of Users or systems providing a high-level overview or statistical summary of DNS activity. The following data is aggregated: • number of DNS queries over time • Queries per second (QPS) metrics • Aggregated by geographical area served by one DNS resolver or ASN • Resolution time averages, percentiles
Anonymisation	refers to the process of transforming personal data in such a way that it can no longer be attributed to a specific individual, either directly or indirectly, irrespective of the use of additional information. Re-identification should no longer be possible
User	Is an individual, natural person, that has chosen to use the DNS4EU Public Resolver because of its reliable operation and enhanced functions, preferably citizen of the European Union, residing in the EU and using the DNS4EU Public Resolver from a place located in the EU. DNS4EU Public Resolvers are aimed to be used primarily by individuals (consumers), not by entrepreneurs in the course of their business.
Backend	is • System for TI propagation • System for logs aggregation and evaluation • System for setting up policies • Works without connection to resolver(s)

Project number: 101095329 21-EU-DIG-EU-DNS, Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union

	• EU hosted on Scaleway
Project Partners	are Whalebone, CZ.NIC, Czech Technical University (ČVUT), Time.lex, deSEC, SZTAKI, Abi Lab, NASK and DNSC
Threat Intelligence Partners	mean national security or cybersecurity research organisations with a public sector mandate (CERTs, CSIRTs, etc.), universities, etc.
Third Party	means any legal entity other than that named in the transparency and privacy notice as being responsible for the operation of the resolver

1. Our commitment

The DNS4EU Public Resolver infrastructure was designed for privacy and security of EU users, and we commit to the following:

1. to operate the service in a fair and non-discriminatory manner;
2. to collect only the information necessary for the proper provision and functioning of the DNS resolution service and research of online threats;
3. to use the information collected solely to improve the performance, security, and user experience of DNS4EU Public Resolver and support the debugging efforts if an issue arises;
4. not to retain or sell or transfer to any Third Party (except as may be required by law), IP addresses or other user identifiers from the DNS queries sent to the DNS4EU Public Resolver;
5. not to combine the data collected from such queries with any other data in any way that can be used to identify individual end users;
6. not to block DNS resolution except for when required by law, enforceable decision of the competent court or other government authority or elected by the User.

2. Data in Public Resolver

2.1. Data collected in logs

Limited DNS query data: The types and categories of data collected by the DNS4EU Public Resolver are:

- DNS query sent by the device,
- Resolver DNS response,

Project number: 101095329 21-EU-DIG-EU-DNS, Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union

- DNS query type
- DNS query timestamp
- Resolver Identifier
- ASN identifier
- Threat type (in case threat is detected)
- Content type (in case content blocking is elected by User)
- Transport protocol
- Query port
- Ttl (time to live)

The DNS query data logs collected for the purpose of the threat research are stored in the Backend (that is installed and hosted in the datacenters controlled and operated within the EU) for up to six (6) months and after that it is deleted.

Aggregated Data, such as total number of queries may be kept indefinitely.

We regard IP addresses associated with its users to be Personal Data (as defined in Article 4 (1) GDPR).

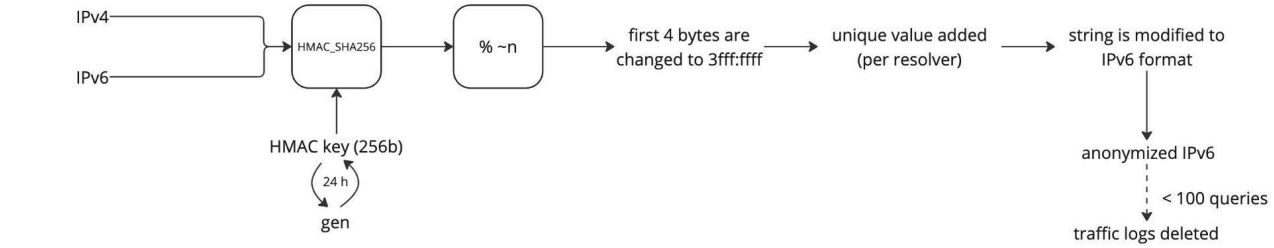
IP Address Anonymization

How is it done?

The IP Address anonymization happens on the DNS resolver.

The IPv4 and IPv6 addresses are processed using the cryptographic hash function HMAC_SHA256, with an HMAC key that is kept in memory only and regenerated daily. The output of this function is then passed through a modulo operation. The value for the modulo is derived from the amount of traffic processed over the past 24 hours by the respective resolver. The modulo value is recalculated daily, along with the rotation of the HMAC key. If traffic data from the past 24 hours is unavailable (e.g., on the first day), the value defaults to 1. After the modulo operation, the first four bytes of the resulting data are replaced with 3fffffff, a standard prefix used in documentation and examples. Subsequently, the resolver ID is included in the anonymized IP address for debugging purposes; however, this does not affect the anonymization in any way. Finally, the string is reformatted into IPv6 notation. To further enhance privacy, for each anonymized IP address, any resulting queries with fewer than 100 requests are deleted.

Project number: 101095329 21-EU-DIG-EU-DNS, Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union



Example of a DNS traffic log with an anonymized IP address

{ "response_time": "2025-04-11T12:12:21.160265Z", "client": "3fff:ffff:7500::34", "server": "86.54.11.1", "class": "IN", "type": "A", "query_port": 33448, "response_port": 53, "query": "dnsperf.com.", "answer": "3.75.10.80", "ttl": 893, "region": "cloud" }

The outcome is a dataset which cannot be reasonably linked anymore to a data subject. Thus, the outcome is an anonymous dataset. It is this dataset which is used exclusively for the purposes of DNS4EU Public Resolvers protection.

2.2. Exceptions

There are only a very limited number of cases in which a non-anonymised IP address is processed. The only activities involving personal data processing are undertaken for the following three purposes:

(i) **Resolving DNS requests (plain resolution)**
Within the execution of DNS request resolution, the client IP address is necessary, since this is where the response must be sent. It is thus essential that the DNS resolver keeps the client IP address in the volatile operating memory for the time necessary to service the client's query (usually milliseconds).

(ii) Accessing the potentially malicious website from warning page
In case the User uses DNS resolution service with one of the additional optional flavors, the service notifies the User he/she is going to access a potentially malicious, illegal or otherwise harmful website (a landing page pops up). If the User decides to attend the website anyway, in such a case the User's IP address is stored by the DNS resolver for up to 24 hours in order to identify the User and not block the access.

(iii) **DNS resolver protection**

In case of an active attack on a DNS resolver, IP address data is processed in order to detect the attacker, i.e. to determine from which IP address(es) the attack(s) is(are) coming, and the volume of data sent, or other attack characteristics. In such cases, the IP address(es) is (are) stored for some time to enable the analysis.

(iv) **Troubleshooting of the DNS resolver**
When the DNS resolver software stops working / terminates itself due to a failure in software or hardware, the state thereof before it happened is saved; i.e. the moment the DNS resolver software stops working, all the IP addresses in the volatile operational memory are recorded on the disk into the snapshot of the memory (the "core dump" as described below), and the technical team works with this data in order to fix the problem.

The processing of IP addresses in these cases is based on our legitimate interest in ensuring the operation, security and safety of DNS communications.

2.2.1. Plain DNS resolution

The client IP address from which any DNS query originates is never stored in non-volatile memory.

The DNS4EU Public Resolver stores the IP addresses from which it receives queries in RAM (volatile random access memory) for the time necessary to service the user's query (usually milliseconds). The data processing is a pure functional result of data being processed in memory; the logs are not retained except in cases of troubleshooting or for DNS resolver protection purposes described below.

Retention period

The data coming from DNS resolution, namely: Electronic communications data, notably an IP address, combined with time stamps and content type descriptions, stays for the duration of handling the DNS query (from milliseconds up to seconds) in the RAM.

2.2.2. Public resolver protection

The actions or observed behaviors that are identified by the algorithm malicious or anomalous trigger the diagnostic process of such incidents, such anomalous incidents being e.g. cyber-attacks against the infrastructure, DDoS attacks, protocol faults, misconfigured or misbehaving clients and malicious exploitation of vulnerabilities in the hardware, software, and networks which constitute our systems. Within the mitigation process data relevant to the diagnosis are collected as well as the IP address connected with the event must be logged. The diagnosis and resolution of such incidents are always provided by dedicated technicians.

Retention period

Data collected under this exception is permanently deleted no later than six (6) months after the end of the attack.

2.2.3. Troubleshooting:

The same procedure as described in the previous section 2.2.2. may also be applied in case of a software crash.

Retention period

In case of troubleshooting, electronic communications data included in core dumps when the system encounters a problem (notably an IP address, combined with time stamps and content type descriptions) collected in logs is retained for up to three (3) months for analysis of the crash only.

3. Security

3.1. Encryption and configuration of DNS traffic

To protect and make the connections / queries private and secure, DNS4EU Public Resolver supports DNS over TLS (DoT) and DNS over HTTPS (DoH), two standards developed for encrypting DNS traffic. This prevents on-path parties from interpreting and manipulating the queries handled via DNS4EU Public Resolver.

3.2. Other measures

Additionally, the resolver performs Domain Name System Security Extensions (DNSSEC) validation, and implements Response Rate Limiting (RRL), which doesn't affect regular users. The DNS resolver uses protection against distributed denial of service (DDoS) attacks.

4. Data sharing

We DO NOT share any information that could identify an individual.

We share limited data as shown in the Example anonymized DNS traffic log in section 2.1. hereinabove with selected Project Partners who train the machine learning models based on this data.

We may share Aggregated Data and/or a subset of anonymized data under strict confidentiality obligations (a written agreement setting up a single purpose of improving User security) with our Threat Intelligence Partners who provide the threat intelligence feeds and analysis in order to protect the Users from malicious attacks. The Threat Intelligence Partners are cautiously selected based on the above purpose.The Aggregated Data may comprise the following information: how many accesses occurred to the malicious domain within a specific period of time, in a specific region (usually being the area served by the respective DNS resolver).

We will make publicly available only general information and reports containing statistical Aggregated Data generated on the basis of the original raw data (e.g. number of threats prevented/DNS queries processed, etc). No original data set will be made available to the public.

5. Correlation of data

We do not correlate or combine data in our possession with data from other sources.

6. Censorship

We do not censor the answers the DNS resolver provides for any purpose other than the blocking of malicious domains associated with phishing, malware, vulnerability exploit, or fraud or, if the User chooses and configures the DNS resolver by himself/herself.

We do not otherwise alter or suppress DNS responses to restrict access to specific internet content through techniques such as DNS manipulation, where DNS queries for certain domains are intercepted and modified to prevent Users from reaching the intended websites.

Users who prioritize privacy and unfiltered access to the internet can use the plain DNS resolution service of DNS4EU Public Resolver.

7. Accidental blocking

We implement allowlisting algorithms to make sure legitimate domains are not blocked by accident. However, in the case of blocking a legitimate domain (or domain intended to be blocked within the respective chosen flavor), we work with the users to quickly allowlist that domain.

Please use our support form (insert link)/ Please email us at the email address set forth in the "Contact information" section below, if you believe we are blocking a domain in error.

8. DNS Resolver User's rights

We are aware of the fact that the User may have the right to access, correct, delete, or restrict the processing of his/her personal information and to receive information about his/her personal data processed by us. As the DNS4EU Public Resolvers do not retain any personally identifiable information about DNS resolver Users, it will most probably be difficult to impossible to effectively handle requests from Users regarding the exercise of their rights.

With respect to these Users' rights we rely on Article 11 GDPR pursuant to which we are not obliged to maintain, acquire or process additional information in order to identify the data subject (User) for the sole purpose of complying with the regulation.

However, if the User voluntarily provides us with additional information to support the exercise of his/her rights under Articles 15 to 20 GDPR, we will not refuse such a request and subject to additional authentication mechanisms, we will exert our best efforts to comply with the request. If you wish to exercise any of these rights, please contact us at the email address set forth in the "Contact Information".

Right to access

As the DNS resolver does not retain any personal data of DNS resolver Users, it is not possible for us as a controller to effectively identify the individual, unless the DNS Resolver User asks and gives additional information to identify him/her.

Right to rectification

When e.g. the IP address is logged within a crash dump, it is logged live and reflects a historical record that cannot change, so rectification is largely irrelevant.

Right to erasure

Provided that the particular IP address is still searchable, it can be deleted. This is expected to be exceedingly rare due to the very short retention period (other than in the very small-scale use case of crash dump logs).

Right to restriction of processing

In case the individual does not want his/her IP address being processed, he/she shall not use the DNS4EU Public Resolvers service.

Right to data portability

Not applicable

Right to object

Project number: 101095329 21-EU-DIG-EU-DNS, Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union

In case the potential User has any concerns regarding the use of the DNS4EU Public Resolver(s) he/she can contact the email address set forth in the “Contact information” section below. The same applies in case of any objections the User may have with regard to his/her data processing. .

Right to not be subject to automated individual decision-making

Not applicable. Insofar as DNS resolution would be considered a form of automated decision-making, it would be “necessary for entering into, or performance of, a contract between the data subject and a data controller” (since the public DNS resolver is accessible under specific contractual terms that the data subject must accept), and thus exempt from this right under Article 22.2(a) of the GDPR

Right to withdraw consent

Not applicable, since the processing is not based on User’s consent. However, the User can stop his/her use of the DNS4EU Public Resolver at any time, in which case the data processing would stop automatically (or, in the unlikely event that their logs were captured in a crash dump, after up to six months).

Contact to the supervisory authority

Should you wish to lodge a complaint or if you feel that our company has not addressed your concern in a satisfactory manner, you may contact the Office for Personal Data Protection, contact details here: https://www.uoou.cz/.

9. Contact information

If you have any concern, questions or comments related to this statement, please send us an email to our DPO at: dataprotection@joindns4.eu

You can also contact us in writing to:

Whalebone, s.r.o,

Jezuitská 13/14 , 602 00 Brno, Czech Republic

Company ID: 05120403, VAT No.: CZ05120403

10. Compliance and Applicable Law

Each DNS4EU Public Resolver falls under the jurisdiction of the Czech regulatory law as well as under the national jurisdiction of each member state in which it is located and operates. Whalebone as operator of DNS4EU Public Resolvers, is subject to the independent supervision of the Czech Office for Personal Data Protection (UOOU).

All activities and practices, including those covered in this DNS4EU Public Resolver Policy comply with the relevant EU laws, especially: GDPR and national data protection laws and regulations, if any.

Project number: 101095329 21-EU-DIG-EU-DNS, Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union

Project number: 101095329 21-EU-DIG-EU-DNS, Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union