Privacy Policy Evaluation

Resolver Reputation 1.0

Date
10 April 2015

Classification
Public

Author
SIDN Privacy Board

Page
1/5

Contact
T +31 26 352 5500
support@sidn.nl
www.sidn.nl

Office
Meander 501
6825 MD Arnhem
The Netherlands

Postal address
Postbus 5022
6802 EA Arnhem
The Netherlands

Policy

Title of policy	Resolver Reputation 1.0
Policy start date	2015-03-17
Date of evaluation	2015-04-10

Purpose limitation

Data Protection Act applicable?

Will any personal data be processed? Will personal data be processed on an automated or semi-automated basis, or will personal data contained in a file be processed manually?

☒ Yes ☐ No

Yes, the submitted form states that the following personal data is processed: IPv4 and IPv6 addresses of all systems that send DNS queries relating to .nl domains (plus the timestamp of the most recently received DNS query).

Purpose

The purpose must be specific, explicitly defined and legitimate.

Is the purpose specific, explicitly defined and legitimate?

☒ Yes
☐ No, insofar as

The submitted form states that the research has the following purposes:

To increase the security and reliability of .nl (and the internet in general) by conducting research into the assignment of reputations to resolvers.

The reputation assignments can then be used to tackle various forms of abuse. Specifically, the intention is to improve the capability to act against 'spambots' (botnet clients that send spam). Spambots are detected by the system on the basis of certain characteristics of their DNS behaviour; their IP addresses are then shared with the Abuse Information Exchange for further processing. That processing entails communication of each IP address to the relevant ISP, who can take appropriate action where warranted.

The ultimate goal of the activities that are relevant to this policy is to reduce the number of PCs in the Netherlands that are infected with spambot malware.

Evaluation:
The purpose is specific, explicitly defined and legitimate.

Legitimate basis

The evaluation must address the proportionality and subsidiarity of the processing (i.e. whether the interest served by processing is important enough to justify any resulting loss of privacy, and whether the purpose could be served by any other, less intrusive means).

Is the legitimate basis clear?

☒ Yes
☐ No

The submitted form states that the legitimate basis for the processing is reasonable interest.

Evaluation:
Reasonable interest is indeed the appropriate legitimate basis (the other legitimate bases referred to in the Data Protection Act are not applicable).
See the Purpose section for details of the reasonable interests served. The research does not significantly compromise the privacy of the users of the processed IP addresses. Furthermore, the research and the sharing of addresses via the AbuseHUB is partly in the interests of the address-holders themselves.

Safeguards and control measures

Purpose limitation

Are there adequate safeguards to ensure that personal data is not used for purposes other than that for which it was obtained?

☒ Yes
☐ No

The submitted form states that access is restricted to SIDN Labs staff. It also states that the data is held on a server, access to which is controlled on the basis of two-

factor authentication (TOTP for SSH and client certificates for web, plus a user name-password combination).

Furthermore, sharing with the AbuseHUB will be subject to the condition that an agreement is in place between SIDN and the AbuseHUB, the content of which corresponds to a processing agreement.

Evaluation:

The Privacy Board recommends that, in addition to the provisions referred to on the form, internal arrangements should be made to ensure that the working methods described are followed in practice (= instructions to relevant personnel).

The agreement with the AbuseHUB provides adequate assurance that sharing will be subject to appropriate safeguards.

Retention period

Is personal data retained for any longer than necessary for the defined purpose?

☐ Yes, data is retained for longer than necessary; corrective measures required.
☒ No

The submitted form states that IP addresses that have not been associated with any recent activity ('recent' implying 'in the last month') will be deleted from the database.

Evaluation:
Given that only IP addresses (minus the associated query data) will be retained, and that retention will be only until one month after the last recorded activity, the stated retention period is reasonable.

Data set limitation

Is the entire data set necessary for the defined purpose, or could a more limited data set be used?

☒ Yes
☐ No; corrective measures required.

The submitted form states that the actual query data is irrelevant to the study and will therefore be excluded from processing. Analysis will be confined to meta-data (whether an MX record is requested, whether the RD bit is set, whether numerous NX domains are involved, etc).

Evaluation:
Only IP addresses are relevant to the purpose of the study. The personal data to be retained therefore consists exclusively of IP addresses. Both in relation to the research and in relation to the sharing of data with third parties, it is important to state more clearly that IP addresses are necessary for realisation of the study's purpose.

Data reliability

What is done to ensure that the gathered data is accurate?

Internally sourced data, as per ENTRADA policy.

Data processors

Who processes the data? Who else has access to the data?

The processed data is gathered (without third-party involvement) by our own systems in the context of normal operational activities (handling DNS queries).

When system output is communicated via the AbuseHUB, recipients are told that we regard the relevant IP addresses as suspect, but make no guarantee regarding the system's results and conclusions.

Data security

How is the data protected against loss and unauthorised processing?

See the information about access control given above.

Evaluation: Given that processing involves IP addresses associated with suspect activity, the level of technical security is considered to be sufficient. In order to ensure adequate organisational security as well, written instructions for the relevant personnel are desirable.

Where sharing via the AbuseHUB is concerned, appropriate provisions should be added to the agreement between SIDN and the AbuseHUB.

Other

Special personal data

Is any special personal data processed?

☐ Yes
☒ No

Inclusion in register

Is the processing recorded in the Processing Register?

☒ Yes
☐ No

Subjects' rights

If the personal data is not obtained from the subjects, but by other means, is the origin recorded?

☒ Yes
☐ No

The submitted form states that the processed data consists of the IP addresses of all systems that send DNS queries to ns1.dns.nl.

Evaluation: The data is therefore obtained by other means, and the origin is recorded.

Retention within EU

Is any data transferred to a country outside the EU?

☐ Yes
☒ No

If 'Yes', advice is required from the Privacy Board.

Conclusion

Evaluation

What is the conclusion of the Privacy Board's evaluation?

The Privacy Board believes that the policy satisfies all applicable statutory and internal requirements.