Privacy Policy Evaluation

Development of DDoS Database

Date	Classification	Page
21 April 2022	Public	1/5
	Author Privacy Board	

Contact
T +31 (0)26 352 5500
support@sidn.nl
www.sidn.nl

Offices
Meander 501
6825 MD Arnhem
The Netherlands

Mailing address
PO Box 5022
6802 EA Arnhem
The Netherlands

Policy

Title of policy	Development of DDoS Database (DDoSDB.nl)
Policy start date	1 February 2022
Date of evaluation	21 April 2022

Purpose limitation

GDPR 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
Why?

The Privacy Board considers that the project will involve the processing of personal data. DDoSDB.nl is the instance of the DDoS-DB database hosted on the SIDN Labs network. The following types of personal data are recorded in DDoSDB.nl:

- *User account information, including the name, e-mail address and affiliation of each user. Only Dutch National Anti-DDoS Coalition (NL-ADC) members participating in the DDoS Clearing House pilot have access. Their IP addresses are placed on a whitelist.*
- *DDoS-DB is used to store and share fingerprints with other coalition members. A DDoS fingerprint is a body of information summarising the characteristics of a DDoS attack, including the source IP address of the attack. That IP address may belong to a compromised third-party system.*

The processed data will include information about identified or identifiable natural persons. Automated processing of personal data is also to be carried out. Hence, the GDPR may be deemed applicable.

Purpose

The purpose must be specific, explicitly defined and legitimate.

Is the purpose specific, explicitly defined and legitimate?

☒ Yes
☐ No, insofar as

The context in which personal data is processed is clearly stated, namely DDoSDB.nl. The purpose of the processing is to enable DDoS attack characteristics to be studied and shared with others in the form of DDoS fingerprints. That will give NL-ADC members a broader view of the DDoS attack landscape, enabling them to defend against attacks more effectively, ultimately helping to make the internet more secure in the Netherlands.

The Privacy Board considers that the Privacy Policy defines the purposes of the processing in specific and explicit terms. The Privacy Board also considers that increasing the effectiveness of attack response capabilities is a legitimate purpose consistent with SIDN's mission and vision. Processing serves a reasonable interest and therefore has a legitimate legal basis in the context of the GDPR.

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 legitimate basis for the data processing is reasonable interest. The research is consistent with SIDN's aim of promoting safe and convenient digital living; it also contributes to internet stability.

The Privacy Board considers that a reasonable interest is served in connection with SIDN's commitment to the security of the .nl domain, as pursued through its membership of the NL-ADC. That interest, and thus the interests of DDoS attack victims, outweighs the privacy interest of any natural person potentially associated with the source IP address of the DDoS attack. The processing is necessary for furtherance of SIDN's reasonable interest.

The Privacy Board considers that the project satisfies the relevant proportionality and subsidiarity requirements. The associated privacy infringement is justified by the purpose.

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 personal data will be processed on SIDN's systems by project personnel, and will be protected by general security measures.

DDoSDB.nl is a closed-user-group web application. It is not publicly accessible. Only NL-ADC members participating in the DDoS Clearing House pilot have access, and their IP addresses are included on a whitelist. All communication between the server and client is encrypted. Users are IP-filtered and required to log in using a password in order to access and/or upload data. The Privacy Board accordingly considers the data security measures to be adequate.

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 fingerprints uploaded to DDoSDB.nl during the development phase will be retained for up to eighteen months. That provides a six-month window for research projects involving a full year of fingerprints. The Privacy Board accordingly considers that the personal data will not be retained for any longer than necessary for the defined purpose.

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 Privacy Board considers that the data set to be used is the minimum required for the fulfilment of the defined purpose of the processing. Processing of the data in question is necessary for the analysis of DDoS attacks and the generation of attack fingerprints.

Data reliability

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

The processed data either is obtained from the subjects themselves (in the case of user account details pertaining to NL-ADC members), or is derived from ADC members' own measurements. ADC members independently process the data to produce DDoS fingerprints using the dissector and the network capture files. A DDoS fingerprint includes the source IP address of the DDoS attack.

Data processors

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

The personal data will be processed on SIDN's systems by project personnel, and will be protected by general security measures. Moreover, DDosDB.nl is a closed user group, whose members have all entered into a contract and are individually responsible for processing IP data to generate fingerprints. All data shared amongst the members is covered by the contract. Finally, a small number of application managers have administrator rights.

Data security

How is the data protected against loss and unauthorised processing?

The personal data will be processed on SIDN's systems by project personnel, and will be protected by general security measures. The personal data will be shared in accordance with SIDN's security policy. Sharing will be by means of secure platforms. All receiving parties will be familiar with SIDN's security policy and must provide the level of security stipulated in that policy. The Privacy Board accordingly considers the data security measures to be adequate.

Other

Special personal data

Is any special personal data processed?

☐ Yes
☒ No

Notification of Data Protection Officer

Has the Data Protection Officer been notified in connection with inclusion in the Processing Register?

☒ Yes
☐ No

The processing is to be recorded if any significant new processing is involved.

Subjects' rights

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

☒ Yes
☐ No

Source IP addresses are obtained from NL-ADC members who upload fingerprints, which are then saved by DDoSDB.nl in the DDoS-database. The origins of the personal data involved are defined in agreements between NL-ADC members.

Retention within EU

Is any data transferred to a country outside the EU?

☐ Yes
☒ No

No data is to be transferred to a country outside the EU.

Conclusion

Evaluation

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

The Privacy Board approves the Privacy Policy for the development of the DDoS database.