European Environment Agency

NOTIFICATION FORM

FOR DATA PROCESSING OPERATIONS

Date of registration: 30.4.2013 Register No: IT11

1. Name of the data processing operation
Internet access logs

2. Data Controller	
Programme or Group:	IDM1
Function:	Helpdesk
Contact person:	Örjan Lindberg; orjan.lindberg@eea.europa.eu

3. Description of the processing operation	
3.1. Area of activity in which the processing is carried out	
Internet access from EEA computers	
3.2. Modalities for the processing operation	
☐ Manual processing	
☒ Automated processing	Access to Internet pages passes through an outgoing proxy server
3.3. Are the Personal data processed by an entity external to EEA ('processor')	
☒	No

4. Lawfulness and purpose of the processing
4.1. Legal basis
The processing operations of EEA's Internet access is based on the provisions of the Service level Agreement entered into between the EEA and EU-CERT.
4.2. Grounds for lawfulness
The data processing is considered lawful because it is necessary for the performance of a task carried out in the public interest on the basis of Regulation (EC) No 401/2009 or in the legitimate exercise of official authority vested in the EEA (Article 5(a) of Regulation (EC) No 45/2001.

4.3. Purpose of the processing
Log files of the accessed Internet pages (web sites/domains) are logged for security reasons only. An infected computer will commonly try to communicate with external resources for various purposes and this type of suspicious access can in that case be traced and the PC found. The background is that EEA has a log management and log security analytics tool provided by CERT-EU called Splunk, that monitors EEA computers access to known suspicious sites via the logs in the outgoing proxy. An outgoing proxy gives the EEA the chance to trace back what has happened and rectify problems. This is only in the event of security breaches such as suspected virus infection alerted from CERT-EU, that the processing will be carried out by IT staff with extended access rights. The data subject is normally contacted and the Data Protection officer may be informed beforehand.

5. Features of the processing operation	
5.1. Categories of data subjects concerned	
EEA Staff and consultants	
5.2. Categories of data	
5.2.1. Data processed in the context of internal telecommunications networks	
☒	Traffic data
☐	Billing data
☒	Directories
☒	Others
5.2.2. Other categories of data	
☒	Logging of access information from Internet resources

6. Retention practice of personal data
Log of your connections (time and IP addresses) are collected in the outgoing proxy. Those log files are kept for 5 weeks before rotated. These logs are at the same time collected and processed in the log management system provided by CERT-EU (Splunk) for detecting security related issues. Retention time for the data/indexes in Splunk is 12-18 months based on the advice from CERT-EU.

7. Personal data processed for historical, statistical or scientific
No personal data are processed for historical, statistical or scientific purposes.

8. Recipients or categories of recipients to whom the data might be disclosed
Data subject and a limited number of relevant IT staff with extended access rights

9. Proposed transfer of personal data to third countries or international organisations	
☐ Yes	☒ No transfer of personal data to third countries or international organisations

10. Information given to the data subjects
Refer to the Overview Data Protection in ICT notice and the privacy statement available on the EEA intranet under work practicality/IT policies/13.

11. Procedures to enable data subjects to exercise their rights
Data subject can exercise their rights through contacting the Internal EEA Helpdesk

12. Time limits for blocking and erasure of the different categories of personal data (*on justified legitimate request from the data subject – Please, specify the time limits for every category*)		
Categories of data	Blocking	Erasure
Any logged data asked for	Usually immediately but at maximum within 5 working days	Usually immediately but at maximum within 5 working days