Processing of personal data in the Finnish Transport and Communications Agency's NIS 2 notification application

Controller	**Controller's contact details**
Finnish Transport and Communications Agency (Traficom)	PO Box 320, FI-00059 TRAFICOM, Finland kirjaamo@traficom.fi telephone +358 29 534 5000 **Contact details of the controller's data protection officer** PO Box 320, FI-00059 TRAFICOM, Finland tietosuoja@traficom.fi telephone +358 29 534 5000 If your message contains confidential, secret or otherwise sensitive content or a personal identity code, please use Traficom's secure email.

Grounds for and purpose of the data processing

The basis for the personal data processing is compliance with a legal obligation to which the controller is subject (Article 6(1)(c) of the General Data Protection Regulation (EU) 2016/679, 'GDPR').

Under section 11 of the Cybersecurity Act (124/2025), an entity shall report a significant incident to the supervisory authority without delay. Supervisory authorities under section 26 of the Cybersecurity Act and section 18h of the Information Management Act (906/2019) are the Finnish Transport and Communications Agency, the Energy Authority, the Finnish Safety and Chemicals Agency, National Supervisory Authority for Welfare and Health, the Centre for Economic Development of Transport and the Environment for South Savo, the Finnish Food Authority and the Finnish Medicines Agency. A significant incident means an incident that has caused or is capable of causing severe operational disruption of services or significant financial losses for the entity concerned and an incident that has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage. An early warning must be submitted within 24 hours and an incident notification within 72 hours of detecting a significant incident. The early warning must include information on the following aspects: (1) the detection of a significant incident, (2) whether the significant incident is suspected of being caused by crime or other unlawful or malicious acts, (3) the likelihood of a cross-border impact and information about forecasting cross-border impacts. The follow-up notification must include the following information: (1) assessment of the nature, severity and impact of the incident, (2) technical indicators of compromise, if available, (3) any updates to information included in the early warning.

According to section 12 of the Cybersecurity Act, an entity must, upon request by the supervisory authority, provide additional information or an intermediate report on status updates concerning the significant incident and progress in handling the incident.

According to section 13 of the Cybersecurity Act, an entity must provide the supervisory authority with a final report on the significant incident within one month of the incident notification or, in the case of a long-term incident, within one month of handling the significant incident. The final report must include the following: (1) a detailed description of the incident, including its severity and impact, (2) the type of threat or root cause that is likely to have triggered the incident, (3) applied and ongoing mitigation measures, and (4) the cross-border

impact of the incident, if any. As regards public administration entities, provisions on the obligation to notify significant incidents are included in section 18d of the Information Management Act.

According to section 15, subsection 1 of the Cybersecurity Act, an entity may submit to the supervisory authority notifications about incidents, cyber threats and near misses other than those referred to in section 11 on a voluntary basis. According to section 15, subsection 2 of the Cybersecurity Act, a supervisory authority must inform the single point of contact referred to in section 18 of notifications of incidents, cyber threats and near misses submitted pursuant to this section. As regards public administration entities, provisions on voluntary notifications are included in section 18f of the Information Management Act.

According to section 17 of the Cybersecurity Act, a supervisory authority must submit the notifications and reports referred to in sections 11–13 and 15 to the CSIRT without delay. If a significant incident has an impact on another European Union Member State, the single point of contact must inform the European Union Agency for Cybersecurity (ENISA) and the affected Member States without undue delay. Upon request, the single point of contact must also submit the notifications and reports referred to in sections 11–13 to the single point of contact of the affected European Union Member State. For this purpose, the single point of contact is allowed to release information about the significant incident to ENISA and the single points of contact in other European Union Member States. As regards public administration entities, see section 18h of the Information Management Act.

According to section 18 of the Cybersecurity Act, the National Cyber Security Centre Finland (NCSC-FI) at the Finnish Transport and Communications Agency acts as the single point of contact referred to in Article 8(3) of the NIS 2 Directive. The task of the single point of contact is to promote cooperation and coordination among supervisory authorities in the performance of their tasks in accordance with the Act. The single point of contact shall submit to ENISA every three months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with sections 11–13 and 15. For this purpose, the single point of contact has the right to obtain anonymised and aggregated data from a supervisory authority. As regards public administration entities, see section 18h of the Information Management Act.

For these purposes, the Finnish Transport and Communications Agency's NIS 2 notification application is used to collect data on significant incident notifications (mandatory notification) and voluntary notifications made by entities. In order to implement this data collection, it is necessary to process the personal data described in this privacy statement.

Data content	
The data undergoing processing	The register processes the information provided by an entity regarding the notified cybersecurity incident. This information may include personal data. Data subjects include the notifier and the persons whose information is entered into the form. The personal data to be processed are the data of persons related to the information security violation communicated to the controller or included in the open fields of the form and in the attached files, such as:

	1) Contact information, such as name, email, telephone number, address, role in the organisation and other contact details provided; 2) Information about the incident and any related personal data; 3) Technical data related to the notifier, such as IP address, browser information and browser version; 4) Any other, including special, information about the data subject that may be provided in the description of the cybersecurity incident, or a personal identity code (e.g. in phishing cases) and information that can be derived from the personal identity code, such as age and sex. The possible processing of special categories of personal data is based on Article 9(2)(g) and possibly Article 9(2)(e) the EU GDPR. Possible processing of the personal identity code is based on section 29, subsection 1 of the Data Protection Act.
Sources of the processed data (where data is received from)	The data to be processed is obtained from the person submitting the notification. The data are provided via a form filled in on the NCSC-FI website. Data can also be obtained from the exchange of messages between the controller and the person filling in the notification form or other contact person in connection with the incident.
Storage period of personal data	Personal data will be stored as long as it is necessary to process the data for the purposes described in this privacy statement, however not for longer than six years from the end of the calendar year during which the data was obtained.

Data processing	
Recipients and categories of recipients of personal data (to whom personal data is disclosed)	Information on incidents, including personal data, is transmitted via the application to the authority supervising the entity in question, to the CSIRT and the single point of contact. The data is not disclosed for direct marketing purposes.
Processing of personal data on behalf of the controller	There are no separate processors, i.e. the personal data is not processed on behalf of the controller.
Transfer of personal data to third countries outside the EU/EEA	The data will not be transferred outside the EU/EEA.
Automated decision-making and profiling	Automatic decision-making or profiling is not used.

Rights related to the processing of personal data
About exercising rights You can exercise your rights by submitting a request to Traficom by email or post. The controller's contact details are listed in this privacy statement under the section 'Controller's contact details'.

The right to lodge a complaint with the supervisory authority

If you believe that your personal data is being processed in violation of legislation, you may lodge a complaint with the Office of the Data Protection Ombudsman.

Office of the Data Protection Ombudsman
PO Box 800, FI-00531 Helsinki, Finland
tietosuoja(at)om.fi
tel. +358 29 566 6700

Right of access	The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed. If processing takes place, the data subject has the right to access the personal data.
Right to rectification	The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate or incorrect personal data.
Right to object	Because processing is based on compliance with a legal obligation, data subjects do not have the right to object to the processing.
Right to restriction of processing	The data subject has the right to obtain from the controller restriction of processing if: - the data subject contests the accuracy of the personal data - the processing is unlawful, but the data subject opposes the erasure of the personal data and requests the restriction of its use instead - the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims - the data subject has objected to the processing of the personal data pending the verification of whether the legitimate grounds of the controller override those of the data subject.
Right to data portability	The data subject has the right to receive the personal data concerning him or her, which he or she has provided to the controller in a structured, commonly used and machine-readable format and the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based on consent or on a contract and the processing is carried out by automated means.
Right to erasure	In situations where the legal basis for the processing of personal data is something other than compliance with a legal obligation, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her. The requested data will be erased unless the controller has a legal basis for refusing to erase the data, such as a legal obligation to retain the data.
Right to withdraw consent	