

Personal data processing of the National Cyber Security Centre Finland's data breach notifications

<p>Controller Finnish Transport and Communications Agency (Traficom)</p>	<p>Controller's contact details PO Box 320, FI-00059 TRAFICOM, Finland kirjaamo@traficom.fi Tel. +358 29 534 5000</p> <p>Contact details of the controller's data protection officer PO Box 320, FI-00059 TRAFICOM, Finland tietosuoja@traficom.fi Tel. +358 29 534 5000</p> <p>If your message contains confidential, secret or otherwise sensitive content or a personal identity code, please use Traficom's secure email.</p>
<p>Grounds for and purpose of the data processing</p> <p>The basis for the personal data processing is the controller's performance of a task carried out in the public interest (Article 6(1)(e) of the General Data Protection Regulation (2016/679) and section 4 of the Data Protection Act (1050/2018)).</p> <p>In accordance with Section 3 of the Act on the Finnish Transport and Communications Agency (935/2018), the task of the National Cyber Security Centre Finland at the Finnish Transport and Communications Agency is to maintain the situational picture of national information security. Pursuant to section 304(1)(7) of the Act on Electronic Communications Services (917/2014), the Finnish Transport and Communications Agency's task is to collect information on data security breaches and threats to online services, communication services, value-added services and information systems, as well as failure and disruption situations of communication networks and communication services. For these purposes, the National Cyber Security Centre Finland's data breach notification form collects information about data security breaches described by the notifiers. In order to implement this collection, it is necessary to process the personal data described in this privacy statement.</p>	

Data content	
<p>The data undergoing processing</p>	<p>The data processed are the information provided by the person filling out the notification form regarding the reported data security breach. This information may include personal information. Registered persons are the notifier and the persons whose information is entered into the form.</p> <p>The personal data processed are the data of persons related to the data security breach communicated to the controller or included in the open fields of the form and in the attached files, such as:</p> <ol style="list-style-type: none"> 1) Contact information, such as name, e-mail, phone number, address, role in the organisation and other stated contact information; 2) Information about the violation and related personal information, such as user account and login information and profile

	<p>pictures of social media or other online environments, or information about the existence of such an ID; financial, bank or payment information, device information such as IMEI code; information about the filing of a report of an offence and related information, such as information about the person who made the report of an offence, information about the police department that received the report and the time of filing; information about any other persons mentioned in the information security breach notification, as well as electronic messages and message forwarding information;</p> <p>3) Technical data related to the notifier, such as IP address, browser information and browser version;</p> <p>4) Other, including special categories, information about the data subject that may emerge from the description of the data breach, or personal identity code (for example, in phishing situations) and information derived from the personal identity code, such as age and gender;</p> <p>5) Information on whether the notifier gives consent to provide information to another authority.</p> <p>The possible processing of special categories of personal data groups is based on Article 9, Section 2, Subsection (g) and possibly Subsection (e) of the General Data Protection Regulation (EU). Possible processing of the personal identity code takes place on the basis of section 29 subsection 1 of the Data Protection Act.</p>
Sources of the processed data (where data is received from)	The information to be processed is obtained from the person making the notification. The information is given on a form that is filled out on the website of the National Cyber Security Centre Finland or by sending the information by e-mail to the CERT e-mail box. Information can also be obtained from the exchange of messages between the controller and the person filling out the notification form or other contact person related to the data security breach situation.
Storage period of personal data	Personal data will be stored as long as processing it is necessary to fulfil the purposes described in this data protection statement, however for a maximum of ten years from the end of the calendar year during which the data was obtained (Act on Electronic Communications Services Section 316 Subsection 4).

Data processing	
Recipients and categories of recipients of personal data (to whom personal data is disclosed)	<p>Data breach information, including personal data, can be exchanged confidentially with other authorities relevant to the breach when required or permitted by law. The person who fills out the form is asked if they consent to the transfer of information to another authority.</p> <p>The data is not disclosed for direct marketing purposes.</p>
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	
<p>About exercising rights</p> <p>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'.</p> <p>The right to lodge a complaint with the supervisory authority</p> <p>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.</p> <p style="text-align: center;">Office of the Data Protection Ombudsman PO Box 800, FI-00531 Helsinki tietosuoja(at)om.fi tel. +358 29 566 6700</p>	
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 personal data concerning him or her.
Right to object	<p>In situations where the processing of personal data is based on public interest, the exercise of official authority vested in the controller or the legitimate interest of the controller or a third party, the data subject has the right to object to the processing of personal data concerning him or her.</p> <p>If a data subject uses his or her right to object, the controller must stop the processing of the personal data, unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.</p> <p>If personal data is processed for direct marketing purposes, the data subject has the right to object to the processing without any specific grounds.</p> <p>In situations where personal data is processed for statistical or research purposes, the data subject may object to the processing on grounds relating to his or her particular situation, in response to which the controller must stop processing the data subject's data, unless the processing is necessary for performing a task carried out for reasons of public interest.</p>

<p>Right to restriction of processing</p>	<p>The data subject has the right to obtain from the controller restriction of processing if:</p> <ul style="list-style-type: none"> - the accuracy of the personal data is contested by the data subject; - the processing is unlawful but the data subject opposes the erasure of the personal data and requests the restriction of their 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.
<p>Right to data portability</p>	<p>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.</p>
<p>Right to erasure</p>	<p>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.</p>
<p>Right to withdraw consent</p>	<p>Insofar as personal data is processed on the basis of the consent of the data subject, the data subject may withdraw his or her consent at any time by notifying the controller of the withdrawal. Withdrawing consent will not affect the lawfulness of processing carried out on the basis of the consent of the data subject before its withdrawal.</p>