

PRIVACY POLICY

Date: December 5, 2025 (point 2, contact person changed)

EU General Data Protection Regulation, articles 13 and 14

1. Data controller	Finavia Corporation Business ID: 2302570-2 Street address: Lentäjätie 3, 01530 Vantaa Postal address: P. O. Box 50, 01531 Vantaa Phone (PABX): +358 20 708 000
2. Contact Person(s) for filing system related matters	Name: Tiina Ranta Title: Vice President Street address: Lentäjätie 3, 01530 Vantaa Postal address: P.O. Box 50, 01531 Vantaa Phone: +358405152359 email: tiina.ranta(at)finavia.fi
3. Data Protection Officer	Data Protection Officer of Finavia Corporation Email: tietosuojavastaava(at)finavia.fi Phone: +358 20 708 2828
4. Name of processing activity	Processing of personal data collected in connection with the security check and guarding duties of Finavia Corporation
5. Purpose of Processing of Personal Data and the Legal Basis for Data Processing	<p>Information on occurrences detected during security checks and guarding duties is recorded in the security check and guarding duty reporting system which may involve processing of personal data.</p> <p>The purpose of the system is to guarantee the legal protection and safety of the employees, to protect the data and property of the employer, employees and customers as well as to prevent and investigate crimes. In situations involving criminal activity or suspected criminal activity, the data is used to clarify the events and identify the individuals involved.</p> <p>The data is processed for the following purposes:</p> <ul style="list-style-type: none"> • To ensure the security of the airport and air travel • To monitor and improve customer experience (including responding to a customer related to the customer feedback process) • For statistical purposes • To meet regulatory obligations • To prevent misuse <p>The legal basis for the processing is:</p> <ol style="list-style-type: none"> a) The processing is necessary to comply with a statutory obligation of the controller (e.g. access control, security check of passengers and their luggage, surveillance and patrols at airports). b) The processing is necessary for the implementation of the legitimate interests of the controller or a third party (guarding and upkeep of public order to the extent not required by law, statistics, quality of customer service, operational development).

	<p>The processing of personal data is based on the statutory obligation of the airport operator to implement airport security measures (item a). The security regulations are based on the Aviation Act (864/2014), the Decree on the Transport of Dangerous Goods by Air (443/2014) and the EU Security Regulation (300/2008).</p>
6. Recipients of Personal Data	<p>Personal data is transferred to a cloud service implemented and maintained by the system provider (ServiceNow Inc.).</p> <p>The personal data collected in the register shall be disclosed in a controlled manner only for the purposes in accordance with this Privacy Policy. Secure data processing and transfer methods shall be followed when disclosing material. Each disclosure of material shall be documented.</p> <p>Data may be disclosed to:</p> <ul style="list-style-type: none"> - A competent authority in specific cases provided for by law, for example, to investigate a crime. - The contact person of an employee's employer, if required by the person's employment relationship. <p>The above disclosure of data is always based on a justified, written and individual request submitted by the recipient.</p> <p>In addition, data can be disclosed to the agents performing the further handling of prohibited items and materials removed from passengers.</p> <p>The data collected in the register shall not be disclosed for commercial purposes.</p>
7. Data Contents of the register	<p><u>Data collection in connection with security screening under certain conditions:</u></p> <p>Passengers:</p> <ul style="list-style-type: none"> • Name of the passenger • Flight number • Flight destination • Passenger type (transfer/local) • Description of the event <p>Employees and other persons subject to security screening:</p> <ul style="list-style-type: none"> • Name of the person • Staff number • User level and validity period of the user level • Description of the event <p>Vehicles:</p> <ul style="list-style-type: none"> • Registration number <p><u>Data collection in connection with guarding duty under certain conditions:</u></p> <p>Passengers:</p> <ul style="list-style-type: none"> • Information pertaining to observations made in connection with guarding duty events is generally recorded without the passengers' personal data; however, in exceptional cases similar personal data may also be recorded as described above

	<p>concerning passengers and vehicles in connection with security checks.</p> <p>Employees:</p> <ul style="list-style-type: none"> Observations made in connection with guarding duties are recorded similarly with those made in security screening of employees. Additionally, log file data pertaining to access control systems is collected. <p>Vehicles:</p> <ul style="list-style-type: none"> Registration number and potentially position data and location <p>Other persons met in the airport area:</p> <ul style="list-style-type: none"> Possible identification of the person without name information (arrival at the airport area, clothing, etc.) The reason for staying in the airport area Event description
8. Data Sources	<p>The data for reports associated with security screening is collected from the data subject him/herself; or in case he or she is unavailable (e.g. in hold baggage screening), the data will be collected from another Finavia IT system based on the unique suitcase tag printed for the baggage by the airline. Event description and possible registration number is collected from the reporter.</p> <p>Data relating to guarding and upkeep of public order can be obtained from security officers, from guards or from third parties (such as the operating airline) or from the access control system of the airport.</p>
9. Transfer of Data to the Countries Outside of the European Union or the European Economic Area	<p>The data in the register shall not be transferred outside the European Union or the European Economic Area.</p>
10. Data Retention Period	<p>Finavia Corporation will retain personal data in accordance with the legislation in force and only as long as necessary for the purposes specified in this Privacy Policy.</p> <p>Reports drawn up in connection with security screening which reveal personal data will be retained for 2 years.</p> <p>Surveillance reports and related information will be retained for 5 years.</p> <p>However, personal data may be stored for a period longer than the aforementioned periods due to the obligations under applicable law.</p>
11. Data Protection Principles	<p>Personal data contained in this register shall be protected by technical and organizational measures against unjustified and/or unlawful access, modification and destruction, or other processing, including unauthorized disclosure and transfer of the data in this register.</p> <p>Data shall be stored in electronic systems protected by firewalls, passwords, and other appropriate technical solutions. Only designated persons employed by Finavia Corporation and other designated persons who need the data to perform their duties, will have</p>

	<p>access to the register. Anyone having access to the data in the register shall be bound by the professional secrecy.</p> <p>Finavia Corporation will comply with strict data security requirements in the management and control of access to its IT systems. Employees who process the data contained in this register as part of their duties will receive regular training and instruction concerning data protection and data security matters.</p>
12. Right of Access and its Implementation	<p>After having supplied sufficient search criteria, the data subject shall have the right to know what data concerning to him/her has been recorded in this register, or that the register does not contain his/her personal data. At the same time, the data controller, shall provide the data subject with information about the regular sources of data, the use of data in the register, and the regular destinations of disclosed data. Refer to section 17. Communications for detailed instructions.</p>
13. Right to Data Portability	<p>After the data subject has submitted personal data concerning him/her to the data controller in a structured, commonly used, and machine-readable format, the data subject shall have the right to transmit personal data concerning him/her to another data controller where;</p> <ul style="list-style-type: none"> a) The data processing is based on the data subject's consent or a contract between the data controller and the data subject, and; a) The processing is carried out by automated means, and; b) If the transmission is technically possible. <p><i>(Right to data portability is not applicable to this processing)</i></p>
14. Right to Withdraw Consent	<p>If the processing of personal data is based on the data subject's consent, the data subject shall have the right to withdraw his/her consent at any time. The consent withdrawal request must be submitted by a personally signed or otherwise comparably verified document, which should be submitted via email to the person indicated in section 2 of this Privacy Policy. However, the processing of data that took place before the withdrawal of consent will remain lawful, even if consent is withdrawn.</p> <p><i>(Right to withdraw consent is not applicable to this processing)</i></p>
15. Rectification, Deletion and Restriction of Processing of Data	<p>The data controller shall, without undue delay on its own initiative or at the request of the data subject, rectify, delete, or supplement inaccurate, unnecessary, incomplete, or outdated personal data in the register for the purpose of processing. The data controller shall also prevent the dissemination of such data if the data could compromise the data subject's privacy protection or his/her rights.</p> <p>At the data subject's request, the data controller shall restrict the processing of data if the data subject has contested the accuracy of his/her personal data, or if the data subject has claimed that the processing of data is unlawful, and has opposed the erasure of the personal data and requests the restriction of their use instead. The data controller shall also restrict the processing of data when the data controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims. In addition, the</p>

	data controller shall restrict the processing of data, if the data subject has objected to the processing of personal data pursuant to the General Data Protection Regulation, and while a determination in pending the verification whether the legitimate grounds of the data controller override those of the data subject. If the data controller has restricted the processing on the aforementioned grounds, the data controller shall inform the data subject before the restriction of processing is lifted. Refer to section 17. Communications for detailed instructions.
16. Right to Lodge a Complaint	The data subject shall have the right to lodge a complaint with a supervisory authority in case Finavia Corporation has not complied with applicable data protection regulations.
17. Communications	<p>The data subject, who wishes to inspect personal data concerning him/her in the manner described in section Virhe. Viitteen lähde ei löytynyt. of this Privacy Policy or to use any other right based on law, must submit a request to this effect either</p> <ol style="list-style-type: none"> by using the Data Subject Access Request form available on the Finavia website https://www.finavia.fi/en/data-protection (recommended), or in a personally signed or otherwise comparably verified document <p>The request in writing (alternative b above) must be submitted to the contact person indicated in section Virhe. Viitteen lähde ei löytynyt. of this Privacy Policy.</p> <p>Finavia Corporation may request the data subject to specify the request and verify his or her identity before processing the request. Finavia Corporation may refuse to execute the request based on the provisions of applicable law.</p> <p>Finavia Corporation will respond to the requests within one (1) month of receiving the request unless there are special reasons to change the response time.</p>
18. Automated Decision-Making and Profiling	The data in the register shall not be used for automated decision-making or profiling the data subjects.
19. Changes to Privacy Policy	Finavia Corporation is continuously developing its business and therefore reserves the right to change this Privacy Policy by posting a notification of changes on its website. The changes to the Privacy Policy may also be based on the legislative changes. Finavia Corporation recommends that the data subjects check the contents of the Privacy Policy on a regular basis.
20. Privacy Policy revisions	<p><u>Sept 11, 2020:</u></p> <p>The security reporting associated to guarding duties has been incorporated in the information system for security check reporting. The contents of this policy document have been revised accordingly. Revised points are marked with vertical lines.</p> <p><u>June 11, 2022:</u></p> <p>The examples of applicability of the legal basis of processing have been supplemented in section 5.</p>

	<p>The data content has been specified in more detail in sections 7 and 8.</p> <p>Data retention periods have been defined in more detail in section 10.</p> <p>Clarification of the applicability of the rights addressed in sections 13 and 14 to this processing.</p> <p>The instructions for contacting the data controller regarding the exercise of the data subject rights are summarized in section 17 of the policy (deleting the same in sections 12 and 15) with no change of the substance except for the added reference to the possibility of using the Data Subject Access Request form on Finavia website.</p>
--	--