

PRIVACY POLICY

Date: 2 November, 2023 (update, section 20 lists amendments)

EU General Data Protection Regulation, articles 13 and 14

1. Data controller	Finavia Corporation [hereinafter "Finavia"] 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: Nina Matilainen Title: Pass Service Manager Street address: Lentäjätie 3, 01530 Vantaa Postal address: P.O. Box 50, 01531 Vantaa Phone: +358 20 708 3244 Email: nina.matilainen(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 register	Finavia permit administration register
5. Purpose of Processing of Personal Data and the Legal Basis for Data Processing	The personal data processed in Finavia's permit administration register consists of personal data required for permits related to the movement of individuals employed by the businesses and authorities operating at airports and their guests, personal data required for permits related to vehicle operation and personal data required for various access rights. Permits, movement of individuals based on these permits and access rights are controlled for the following purposes: to guarantee the legal protection and security of employees; to protect the data and property of the employer, employees and customers; to prevent and investigate crimes; to monitor whether production processes are running appropriately; and to prevent or investigate situations that pose a danger to security, property or production processes. Processing includes the processing of access rights and monitoring of access for persons with electronic access control tags in relation to the following: - access-controlled doors, - access to facilities and areas, and - access to other services only available to employees working at the airport. <u>Personal data can be processed for the following purposes:</u> - enabling access control by Finavia and Finnair Corporation in order to ensure the security of the airport and air travel; - maintaining client relationships (e.g. the LUSO application, invoicing of services and enabling access to the airport extranet service);

	- enabling fees for services used via electronic access by employees working at the airport to be invoiced from the operator with whom the contract concerning the use of the services has been made; - fulfilling requirements from authorities (to ensure compliance with legislation); - preventing abuse (including prevention of unauthorised access); - monitoring the rights of known suppliers of airport supplies (to ensure that they have the permits required to carry out the operations in question and that the permits are valid). <u>The legal bases of the processing are as follows:</u> a) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g. employment relationship with Finavia and the related ID card; order/contract pertaining to services offered by Finavia to its customers, such as the LUSO application; etc.). b) Processing is necessary in order for the data controller to meet a statutory obligation (e.g. permits related to accessing security-controlled areas and controlling access to these areas). c) The data subject has consented to the processing of their personal data for one or several specific purposes (to conduct a security clearance background check, including criminal records, as a prerequisite for obtaining an ID card and to enable reliability monitoring). d) Processing is necessary for exercising legitimate interests pursued by the data controller or by a third party (e.g. the right to access services provided by Finavia that are not required by law; invoicing of service fees; and the disclosure of information on the data subject's permits to a third party to carry out the security management required by law or their legitimate interest). e) The data subject has consented to the validity of their right to drive being verified from the register of the authority responsible for driving licences. The processing of personal data (item b above) is based on the airport operator's statutory obligation to implement access control at airports. Airports are required to control access to the security restricted area (SRA) of the airport and the critical part of the security restricted area (CSRA) pursuant to Regulation (EC) 300/2008 (security regulation) and Commission Implementing Regulation (EU) 2015/1998, and to designate known suppliers pursuant to Regulation (EU) 2015/1998, point 9.1.3. The legitimate interests pursued by the data controller or by a third party, as mentioned in item d) above, are: - using the electronic identification, which is mainly intended for access control purposes, to enable access to other services provided by Finavia and to control the aforementioned access so that Finavia can carry out its business efficiently, - invoicing customers for the service fees, and - concerning the disclosure of data described in section 6:
--	---

	○ the compulsion of a third party to manage the validity of access rights to their premises in the Finavia Access Control System in accordance with the regulations, and ○ the ability of both the data controller and a third party to effectively monitor the validity of permits of employees who need permits and to direct persons who need permits to apply for the permits in accordance with the process defined by Finavia.
6. Recipients of Personal Data	Personal data collected in the register is disclosed in a controlled manner, solely for the purposes pursuant to this privacy policy. Secure methods of data processing and transfer are employed when disclosing materials. Part of the data in the register is retained and processed on servers administered by data processors providing information technology services. Data is continuously transferred to those servers. In addition, data is disclosed: – regularly to Finnair Corporation to the extent that Finnair is responsible for implementing the access rights of individuals (at points where access is controlled by Finnair), – on request to a person indicated by the employer as the contact person (e.g. in matters related to permit applications or validity), and – on request to Fintraffic Air Navigation Services Ltd for validity control of permits entitling access to operational air navigation facilities and – on request to the sub-contractor company handling the invoicing of the data subject's employer (e.g. the name of the person ordering the temporary permit or the time of the visit). The contact details of a company's permit contact person or persons may be disclosed to those who express a need to obtain an ID card or a permit in relation to movement within the airport, in order to direct the individual to apply for the ID card or permit via the relevant application process. The data can be transferred to system vendors of the register in connection with maintenance or testing in relation to technical development that cannot be performed without actual register data (systems which are not based on cloud services). The data also be disclosed to a competent authority in cases separately mandated by law, e.g. to investigate a crime, based on a prior written request from the recipient Data collected in the register shall not be disclosed for commercial purposes.
7. Data Contents of the register	<u>Data subject categories:</u> • employees who have already applied for permits; • representatives of the employer (permit contact persons, company security representative and persons authorised to sign on behalf of the company); • accompanied persons (guests/employees); • vehicle owners/drivers.

	<u>Data collected for each data subject category:</u> Employees (including but not limited to): • name • national identification number/date of birth; • photograph; • personal identification number; • access control tag number; • nationality; • contact details; • title; • employment period; • education history; • security clearance data; • data regarding permits and access rights which have been applied for and/or granted; • admonitions, if applicable; • history of living abroad in the past five years; • electronic tag reader data – time and target of access control; • copy of security clearance application. Companies/employers (including but not limited to): • name, contact details, national identification number, contract for use and education history of the employer's representative/permit contact person, company security representative and person authorised to sign on behalf of the company. Accompanied guests/employees (including but not limited to): • name; • company/employer; • national identification number/date of birth; • permit data. Vehicles of the vehicle owners/drivers: • vehicle data (e.g. registration number).
8. Data Sources	Data recorded in the register is obtained from various permit applications completed by the employer's representative/permit contact person or by the employee, from contract information related to permits and from authorities, training systems, customer data, Finavia's head of security and from technical reader devices. In addition, Finnair Corporation provides data on the access rights related to the ID cards for its flight crew. This data is obtained via a technical data transfer channel in order to implement the flight crew's access rights in the access-controlled facilities administered by Finavia.
9. Transfer of Personal Data to Countries Outside of the European Union or the European Economic Area	Personal data shall not be disclosed or transferred to countries outside of the European Union or European Economic Area.
10. Data Retention Period	Permit recipients' data and applications are retained for the remainder of the current year + 6 years starting from the time when the employee or guest returned the permit, or until the remainder of the current year + 6 years following the permit end date.

	The data of the permit contact person is retained in the system for as long as they act as the contact person and until their replacement has been appointed. The data of the permit contact person is retained in applications for as long as each application completed by them must be retained. We will take reasonable measures to keep the personal data we possess accurate by deleting unnecessary data and updating outdated data. Data will be entered in the register as obtained from the data subject or from another source mentioned in section 8 and will be updated to reflect the information provided by the data subject to the data controller.
11. Data Protection Principles	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. 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 access to the register. Anyone having access to the data in the register shall be bound by the professional secrecy. 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 as part of their duties will receive regular training and instruction concerning data protection and data security matters.
12. Right of Access and its Implementation	After having supplied sufficient search criteria, the data subject shall have the right to know what data concerning to him/her has been recorded, or that his/her personal data is not processed. At the same time, the data controller shall provide the data subject with information about the regular sources of data, the use of data, and the regular destinations of disclosed data. Refer to section 17. Communications for detailed instructions. Pursuant to Section 34, subsection 1 of the Data Protection Act, the data controller has restricted the data subject's right of access to their own data in accordance with the EU's General Data Protection Regulation, in so far as it applies to data concerning the person's access history, obtained from the readers used for access control.
13. Right to Data Portability	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; 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.

	The aforementioned right to data portability does not apply to the data in this register, because the data has not been received from the data subject in a machine-readable format.
14. Right to Withdraw Consent	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. As required by the Security Clearance Act, the data subject has consented to the security clearance, the related reliability monitoring and data collection and the verification of the data given in the application. The consent in question has been submitted to the competent authority for the purpose of conducting the security clearance. Finavia processes the security clearance application, data related to the security clearance certificate received from the competent authority and data related to reliability monitoring. With regards to Finavia, the processing of this data is based on a statutory requirement. In the case that the data subject withdraws their consent given in order to enable reliability monitoring, the security clearance certificate and the permits granted can be revoked, as the statutory requirements for maintaining the validity of the permit are no longer met. The processing of data related to the security clearance can only be terminated after the permits and the related ID card and access control tags have been returned.
15. Rectification, Deletion and Restriction of Processing of Data	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. 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 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 for the aforementioned

	grounds, the data controller shall inform the data subject before the restriction of processing is lifted. The data subject's rights to deletion or restriction of processing are not applicable to the data contained in this register, as the processing is based on the controller's statutory obligation. The data will be deleted at the end of the retention period specified in section 10.
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	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 - 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 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. 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. 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.
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 or in another appropriate way. 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. Changes made to previous versions of the document	<u>Date: Jun 23, 2021</u> Sections 5 and 6 supplemented concerning disclosure to Fintraffic ANS Ltd of information regarding the validity of certain permits. The description of transfers and disclosures of data in section 6 re-structured for a more logical sequence. Content revision due to the increased number of out-sourced service providers. <u>Date: 2 November, 2023</u> In section 5, the description of the legitimate interests of the data controller or a third party in relation to data disclosures has been supplemented.

	In section 6, addition of a description concerning the disclosure of data to an external company used by the data subject's employer that handles its invoicing. Added access control readers to the description of data sources in section 8. Information (which was previously given in sections 12, 15 and 17) concerning the alternative ways for the data subject to submit requests was concentrated in section 17 Communications. Also a recommendation for the data subject to use the Data Subject Access Request form available on Finavia's website was added into section 17 when access to one's personal data is desired. Added to section 19 the text "<i>or in another appropriate way</i>".
--	--