PRIVACY STATEMENT
Article 12 of the General Data Protection Regulation (679/2016)

Date of issue
3 October 2022

D/701/00.06.02.01/2022

1 Data controller	Name National Audit Office of Finland
	Address Porkkalankatu 1 FI-00180 Helsinki
	Other contact details (e.g. phone number during office hours, email address) Tel. +358 (0)9 4321
2 Contact person for register-related matters	Name Jaakko Eskola
	Address Porkkalankatu 1 FI-00180 Helsinki
	Other contact details (e.g. phone number during office hours, email address) Tel. +358 (0)9 432 5713
3 NAOF's Data Protection Officer	Name Tuomo Salminen
	Address Porkkalankatu 1 FI-00180 Helsinki
	Other contact details (e.g. phone number during office hours, email address) tuomo.salminen@vtv.fi
4 Name of register	Financial audit data
5 Purpose of personal data processing and legal basis for the processing	It is a statutory task of the National Audit Office of Finland (NAOF) to audit the legality and appropriateness of the state's financial management and compliance with the state budget. The statutory obligation of the National Audit Office to conduct audits is based on section 90 of the Constitution of Finland, and its tasks and the limits of its competence are laid down in the Act on the National Audit Office. The NAOF ensures that the state budget and the key provisions on the state's financial management are complied with, and that the reports provide true and fair information on the revenue, expenditure and financial position of the central government and its agencies and institutions. Financial audits are conducted on all central government accounting offices, with the exception of Parliament, the Finnish Institute of International Affairs and the National Audit Office, as well as on the final central government accounts and three state funds. In order to carry out this task, financial audits process data on the audited entities, and the data may include personal data. The processing of personal data is related directly to the execution of financial auditing, and the data is needed in the audit of central government revenue and expenditure or processes related to them. The NAOF has the right to obtain the information it needs to perform its duties from public authorities and other entities audited by it. Based on its audit task, the NAOF is provided with data sets that contain various fields at row level. The data content has been limited to the field data directly needed to achieve the audit objectives. In principle and as a rule, the data consists of public information related to central government revenue and expenditure. Audits or measures cannot be carried out or it is not possible to achieve the same results in audits without personal data, e.g. audits of access rights or identification data that is necessary for the examination of deviations. Personal data as such is not audited. However, auditing does not require the identification of the data subject in the case of all financial audit data, i.e. the identification of the data

	subject is relevant only in certain situations. As a rule, the persons included in the data are persons working in or receiving salaries or fees from central government accounting offices. It is necessary to examine rows and fields containing personal data, as it makes it possible to conduct a comprehensive audit and find deviations. The processing of personal data collected in connection with financial audits has a lawful basis and purpose under the EU's General Data Protection Regulation (2016/679). The NAOF does not process personal data belonging to special categories. All data that is processed is linked to the above-described audit task of the National Audit Office. Data is not processed for the purpose of automated decision-making or profiling persons.
6 **Data contained in the register**	1. General ledger data General ledger data includes the general ledger transactions of all central government accounting offices subject to financial audits by the National Audit Office. Personal data may be included in the specification field on the transaction row. The specification field describes the content of a book entry and also provides information that enables an audit trail. The personal data in the specification field may mainly be a name, which as such does not usually make it possible to identify the person. 2. Data produced from the Handi system The data produced from the Handi system consists of approximately 50 separate data sets. The data contains information on the transactions of the central government's *From need to payment* process at different stages of the processing. Personal data may be included in the row data of transactions as information on the bank account, email or user ID. 3. Bank statement data Bank statement data includes all transactions in the central government's revenue and expenditure accounts. Personal data included in it consists of a person's name and bank account. Payments made by a private person may contain personal data provided by the payer in the message field in order to identify the payment if the payer has not provided a reference number. 4. Payroll data Payroll data consists of data on the salaries and fees of the employees of the government agencies subject to financial audits by the National Audit Office. The data includes data per salary period on the employee's salary in euros and pay components. The data can be combined in full with personal data, and its personal-data-like nature is taken into account in its utilisation and processing in audit activities. 5. Data produced from the time management system The data produced from the time management system contains information on the remuneration and bonuses paid on the basis of working hours to the employees of the government agencies subject to financial audits. The data includes transactions especially in the case of agencies with material compensations transferred from the time management system to the payroll system. The data can be combined in full with personal data, and its personal-data-like nature is taken into account in its utilisation and processing in audit activities. 6. Holiday pay liabilities data The data on holiday pay liabilities consists of the holiday pay liabilities of employees of the accounting offices subject to financial audits by the National Audit Office. Holiday pay liabilities are audited based

	on a sample, and the sample data contains personal data. The information contained in the sample can be combined in full with personal data, and its personal-data-like nature is taken into account in its utilisation and processing in audit activities. 7. SAP Connector data The SAP Connector data consists of the SAP FICO data generated by the tests used in financial audits. Information regarded as personal data is saved on the central government's person vendors and transaction handlers in connection with the central government's financial transactions. 8. SAP HCM data The SAP HCM data consists of information on which the payroll computation of the accounting offices audited by the National Audit Office is based, with the exception of time management and the information on salary reductions recorded directly in CGI Salaries. The data contains background information for salary computation, such as information on the basic part of pay as well as certain process-related information. The information can be combined in full with personal data, and its personal-data-like nature is taken into account in its utilisation and processing in audit activities. 9. Data produced from the access rights of the Handi system The access rights management data of the Handi system consists of the Handi users' user IDs, user groups and email addresses. 10. Data produced from the access rights of the Pointti system The access rights data of the Pointti system consists of the Pointti users' user IDs, user groups and email addresses. 11. Data produced from the access rights of the Nomentia system The access rights data of the Nomentia system consists of the Nomentia users' user IDs, user groups and email addresses. 12. Data produced from the access rights of the Kieku system The data produced from the access rights of the Kieku system consists of the Kieku users' user IDs, organisational information and work role information. 13. Data produced from the access rights of the M2 system The access rights data of the M2 system consists of the M2 users' name, register-specific personal ID number and organisational information.
7 **Regular data sources**	The regular data sources are described in section 6 above.
8 **Information on the transfer of data to third countries and on the safeguards applied (incl. information on the existence or absence of the**	Data is not transferred to third countries. Nor is the data processed through an open interface.

Commission's decision on the adequacy of data protection), and means of obtaining a copy of them or information on their content	
9 **Personal data retention period**	The data described above is used for carrying out the statutory task of the National Audit Office. The data is retained in compliance with the general guidelines for the retention of audit data. The data referred to in section 1 (General ledger data) is retained for a period of ten years and other data for a maximum period of six years (1+6).
10 **Register protection principles**	The data security of the register and the confidentiality, integrity and usability of personal data are ensured by appropriate technical and organisational measures. The data is processed in the operating environment of the National Audit Office. The data described in section 6 may only be processed by persons working with financial auditing at the National Audit Office. The persons working with financial auditing have access to the central government's accounting transaction data described above (1 General ledger data) in the scope required for their duties. The other types of data described above are processed in a centralized manner. Access to them is limited to the persons who carry out audit activities based on them. All persons working with financial auditing do not have access to this data.
11 **Right to access and rectify the data**	The data subject has the right to access the data stored on them in the register. To access the personal data stored in the register, the data subject can submit a request to the National Audit Office's registry. When making the request, the data subject must provide proof of their identity. Based on the information content of all data, it is not possible to identify the data subject unambiguously. Where personal data enabling the identification of a data subject is not necessary in view of the purpose of processing personal data, the General Data Protection Regulation (GDPR) does not oblige controllers to store, obtain or process such additional information solely in order to comply with the GDPR. However, the data subject may provide further information for identification purposes. The information content of the data sets submitted to the National Audit Office is owned by the audited agencies. Where necessary, the National Audit Office may transfer a request for information to the relevant agency for decision.
12 **Right to erasure**	The information content of the data processed by the financial audit function is owned by the audited accounting offices. The National Audit Office cannot edit this information on the basis of its own statutory audit task.

	The National Audit Office may refer any request for erasure of data to the agency in question for decision. The data subject can request erasure of personal data from the register by submitting a request to the National Audit Office's registry. When making the request, the data subject must provide proof of their identity.
13 **Right to restrict the processing**	The data subject has the right to demand that the controller restrict the processing of data if • the data subject disputes the accuracy of the personal data; • the processing is contrary to law, and the data subject objects to the erasure of their personal data and demands instead that its use be restricted; • the controller no longer needs the personal data in question for the processing purposes, but the data subject needs it in order to prepare, present or defend a legal claim. The National Audit Office processes the personal data described above in its audit activities in order to carry out its task in the public interest. The data subject can request restricting the processing of personal data in the register by submitting a request to the National Audit Office's registry. When making the request, the data subject must provide proof of their identity.
14 **Right to lodge an appeal with the supervisory authority**	The data subject has the right to lodge a complaint with the supervisory authority if the data subject believes that the processing of their personal data infringes applicable data protection laws.