Data protection and data management guide

Purpose of the guide

The purpose of the guide is that you, as a client of the Hungarian State Treasury (hereinafter referred to as the Treasury), or a person otherwise involved in the data processing of the Treasury, present in a general, concise and comprehensible manner the data management of the Treasury, the essential issues that are important to you, may be related to the protection of your personal data.

This guide will be published with the content in accordance with the applicable regulations of the Treasury on data management. The Treasury reserves the right to change this guide. The Treasury publishes information on any changes.
If you have any question with this guide or the data managment of the Treasury, please write your question to the following e-mail address adatvedelem@allamkincstar.gov.hu and our colleague is answer for you.

Data of the data manager

Data menager

name:	Magyar Államkincstár
place of residence:	1054 Budapest, Hold utca 4.
postal address:	1909 Budapest
e-mail address:	info@allamkincstar.gov.hu
phone number:	1811
homepage:	http://www.allamkincstar.gov.hu/

Data protection officer:

name:	Dr. Dobai Bálint
postal address:	1909 Budapest
e-mail címe:	adatvedelem@allamkincstar.gov.hu

Concepts

Explanation of the most common concepts:

Personal data
Any information relating to an identified or identifiable natural person ("affected"). Identified natural person is a natural person who, directly or indirectly, in particular an identifier, such as name, number, positioning data, online identifier, or physical, physiological, genetic, intellectual may be identified on the basis of one or more factors relating to its economic, cultural or social identity.

Special data
All data belonging to specific categories of personal data, personal data referring to racial or ethnic origin, political opinion, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data intended to uniquely identify natural persons, health data and natural personal data relating to the sexual life or sexual orientation of persons.

Affected
A natural person identified or identifiable by any information.

Data management
All operations or operations performed on personal data, data files in an automated or non-automated manner such as collection, recording, systematization, distribution, storage, transformation or alteration, querying, access, use, communication, transmission, distribution or other means by way of alignment, interconnection, restriction, deletion or destruction.

Data manager
It is a natural or legal person, public authority, agency or any other organization that determines the purposes and means of the processing of personal data independently or with others; if the purposes and means of data management are defined by EU or Member State law, the specific aspects of the appointment of the controller or of the controller may be determined by Union or national law.

Data processor
It is a natural or legal person, a public authority, an agency or any other organization that processes personal data on behalf of the controller.

Consignee
A natural or legal person, public authority, agency or any other organization with or with whom personal data are disclosed, whether or not a third party is. Public authorities which have access to personal data in accordance with EU or Member State law in the context of a specific investigation shall not be considered as a recipient; the handling of such data by these public authorities must comply with the applicable data protection rules in accordance with the purposes of the data management.

Third party
The natural or legal person, public authority, agency or any other organization which is not the same as the data subject, the controller, the data processor or the persons authorized to manage personal data under the direct control of the controller or the processor.

The consent of the affected
Affected of the will of the data subject on a voluntary, concrete and appropriate basis and by means of a statement expressly expressed by the relevant statement or confirmation that he or she agrees to the processing of personal data concerning him or her.

Data protection incident
Damage to security that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data transmitted, stored or otherwise processed.

Major legislation on data management

Legislation containing general data protection provisions:

- REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (general data protection Regulation - GDPR)
- Act CXVII of 1995 on Personal Income Tax (hereinafter referred to as: Income Tax Act)
- Act XC of 2017 on Criminal Procedure law
- Act LIII of 1994 on Judicial Enforcement law
- Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation Activities law
- Act XXXVIII of 2010 on Probate Proceedings (hereinafter referred to as: PP Act)
- Act CXII of 2011 on Informational Self-determination and Freedom of Information (hereinafter referred to as: Info Act)
- Act V of 2013 on the Civil Code (hereinafter referred to as: Civil Code)
- Act XXV of 2023 on Complaints, Public Interest Disclosures, and Rules Related to Reporting Misconduct Act CCXXII of 2015 on general rules for electronic administration and trust services
- Act CL of 2016 on general administrative regulation
- Act CXXX of 2016 on Code of Civil Procedure
- Act I of 2017 on Administrative Proceedings
- Act LXXVIII of 2017 on Atterney Activity
- Act CLIII of 2017 on Enforcement Procedures to be Implemented by the Tax Administration
- Government decree No. 310/2017. (X.31.) on Hungarian State Treasury

The main legislation containing data management provisions concerning the investment services and ancillary services activities of the Treasury:

- Act CVIII of 2001 on certain issues of electronic commerce services and information society services
- Act CXX of 2001 on the Capital Market
- Act CLXXIV of 2005 on Supporting Young People's Life Start
- Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities
- Act LXXXV of 2009 on Provision of Payment Services
- Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing
- MNB Decree No. 35/2017. (XII. 14.) on the Execution of Payment Transactions

IT and physical security and property protection of the Treasury:

- Act L of 2013 (hereinafter: Ibtv.) on Electronic Information Security of State and Local Government Bodies
- Decree of the Ministry of the Interior 41/2015 (VII. 15.) (hereinafter: Ibtv vhr.) on technological security and requirements for secure information devices and products, as well as for classification into a security class and security level, as defined in Act L of 2013 on the electronic information security of state and local government bodies.

– Act CXXXIII of 2005 (hereinafter: the Property Protection Act) on the rules governing the protection of persons and property and the conduct of private investigations

Legal basis for data management

The legal basis for data management determines the legal authority of your personal data to be transferred to the Treasury and on what basis the Treasury can manage it. The legal basis may be multiple.

In most cases, the legal mandate is related to the public service provided by the Treasury, and the relevant legislation prescribes which data, for what purpose, under what conditions and for how long the Treasury can manage. These are cases of mandatory data processing under Article 6 (1) (c) and (e) GDPR.

The data management of contracts concluded between you and the Treasury (for example for the provision of payment services) is based on the contract itself, and the data processing is necessary for the performance of the contract or for taking action at your request prior to the conclusion of the contract. This is a case of data management based on a contract under Article 6 (1) (b) of the GDPR. For this case, if the Treasury manages the data on the basis of a contract with a state agency that has a contract or sponsor relationship with you.

The treasury contracts may also contain your personal data in cases where you are neither a client nor a contractual partner of the Treasury (for example personal data of persons registered as contract agents). The managing of these data is allowed to the extent required by the relevant statutory regulations, for example because the person involved in data management is the employee of the Treasury contractor. These are cases of data management related to the contract, where the legal basis for data management - based on the NAIH / 2018/2570/2 / V of the National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) - is the legitimate interests of the contracting parties as well as the processing of the data by the contracting party, it also provides the basis for the performance of an employment contract between its employee.

In addition to the above cases, the Treasury does not handle personal data in connection with its public task or contracts, but provides services that you can freely, without influence, voluntarily, without having to enter into a contractual relationship (for example newsletter services, some customer service convenience). In such a case, your prior, informed, voluntary and explicit consent will provide the legal basis for the data management. This is a voluntary contribution based on Article 6 (1) (a) GDPR.

With regard to the electronic monitoring systems of the Treasury's property protection, the Property Protection Act provides. requirements. In this respect, the legal basis for the processing of data by the Treasury for the performance of public tasks is provided for in the Ibtv. and Ibtv vhr. the requirement to provide physical protection in accordance with. The Treasury shall issue a preliminary and clearly perceptible warning sign and textual information on the fact that it is using an electronic monitoring system in the customer services area.

Purpose of data management

In the case of the performance of a task in the public interest and the exercise of public power, the legal status of the Treasury determines the legal basis for data processing.

In the case of mandatory data management, the purpose of the data management, which applies to the case or activity by which you contacted the Treasury, is determined by the law. The Treasury may manage your data solely for the purposes this determined.

In the case of contract-based data management, the Treasury manages your data only for the purpose specified in the contract (eg provision of investment services) for the purpose of fulfilling the contract with you.

In the case of contract-related data management (for example contact data), the Treasury manages the data solely for the purpose of the contract.

In the case of data management based on voluntary consent, you will be given detailed information about the purposes of data management before you give the permission and your data is to be processed. The Treasury manages your data solely for the purpose of your prior knowledge and consent to this information.

In some cases, the same data may be processed on the basis of different legal bases, in which case the objectives defined by one of the legal bases will be extended to the objectives set by the other legal basis. For example, on the basis of its voluntary consent, the data provided and recorded for the purposes set out in the contribution may be managed by the Treasury for the purpose of fulfilling a statutory obligation (for example investigation).

The purpose of processing the data provided to the Data Controller in relation to its government securities distribution activities is to identify customers, assess compliance, maintain contact, and fulfill the tax obligations of the Data Controller concerning the customer.

Due to the specific legal status of the Data Controller, it is authorized to manage the personal identification data, nationality, address, and tax identification number of Hungarian children born in Hungary after December 31, 2005, to enforce the objectives defined in Act CLXXIV of 2005 on the start-of-life support for young people.

The Data Controller does not perform profiling in relation to its government securities distribution activities, and its data processing is not for direct business acquisition purposes.

Circle of the managing data

Circle of the managing personal data
- mandatory data managing is required by law;
- in the case of contract-based and contract-related data management, the subject of the contract itself determines what personal data is required to fulfill it;
- Data management based on voluntary consent also takes care of the data necessary for the realization of the objective, which is included in the detailed information provided to you.

The Treasury manages the data belonging to the following data groups in its investment service and supplementary service activities:

a) Identification data of the Affected (in accordance with the relevant provisions of Pmt);
b) Transaction data, invoice and service features related to the performance of the concluded contract;

c) Data required for the fulfillment of preliminary due diligence and anti-money laundering obligations, as well as the results of the related compliance test;
d) Contacting the Affected, contact information for information related to the contract.

The Treasury primarily manages the following data of the Affected:

a)	b)	c)	d)
surname and first name	place, date and amount of the transaction	habits of transactions	phone number
name of birth	purchased government securities	financial knowledge	e-mail address
mother's name of birth	service used	property situation	postal address
place and date of born	balance information	educational attainment	
nationality	tax ID number	investment data	
address, place of residence	copy of tax ID number	Knowledge regarding politically exposed person (PEP) status	
number of address card	Payment reference number of the client's payment account	Information on the source of funds and assets	
number of identification document, expiration date, type			
copy of adress card and identification document			
(face)image			
signature pattern			

The exact information handled during investment service and ancillary service activities is contained in the Data Manager current Term of Business, as well as the individual contracts, orders, and other documents generated during the execution of the contracts.

The Data Manager handles personal data primarily for the purpose of preparing contracts or concluding a contract.

The Data Manager handles special data in limited cases, under strict conditions and only if the Affected expressly agrees to the data management, or if the data management is necessary for the performance of an international contract promulgated by law, or the enforcement of a fundamental right guaranteed by the Fundamental Law, as well as national security is required by law to prevent or prosecute criminal offenses or is ordered by law for a public interest purpose.

Transfer of personal data

Legislation on mandatory data management may require the Treasury to transfer data. In this case, the legal basis for the transfer is the legal obligation that requires it.

In the case of contract-based data management, depending on the subject of the contract, but only the data may be transferred for the performance of the contract, for which you will be informed during the conclusion of the contract (for whom, for where and for what purpose).

In the case of data processing based on voluntary contributions, the transmission of data may be exceptionally necessary, in which case this is included in the information prior to your consent**.**

The Data Controller carries out data management and processing within its own organization. However, in the context of outsourcing activites related to government securities distribution, data transfer takes place in accordance with the relevant legal provisions. The scope of the outsourced activities and the entity performing the outsourced activities are specified in Appendix No. 8 of the current Terms of Business.

The recipients of the data transfer
The Personal Data shall be transmitted by the Data Manager only if the Affected has given his consent, or is permitted by, or stipulated in the Contract, or the law.

Requests for data from the Data Manager are provided for by only statutory organizations they are entitled only to ensure the performance of their statutory duties (for example: investigative authority, prosecutor's office, court, national security service). The Data Manager's confidentiality obligation towards these organizations does not exist within the applicable legal framework, thus it also transfer personal data about the Parties.

The scope and types of data management to be provided in this circle shall be determined by the body or organization ordering the data processing within the relevant legal framework for the duration of the data management, and the possibility to notify the customer of the data transfer.

The Data Manager shall also be entitled to forward the personal data of the Affected

a) in that case transfer the data to the Government Debt Management Agency Zrt (independent data manager) like third party (organization), if the Government Debt Management Agency Zrt. for the evaluation of the fulfillment of the Distributor Agreement, the Client's subscription form, so the Client's personal data is requested in writing from the Data Manager;
b) forward to another investment service provider (independent data manager) if the Client requests the transfer of the securities registration account to another investment service provider.
c) to the intermediaries of the Treasury, in the event that it is necessary in connection with the use of investment services and additional services provided by the Treasury or the performance of contracts concluded with the Treasury in the course of their intermediation activities.

The following organizations will be the recipients of data transfer, of these, of course, only the ones for which the statutory rule, contract or your consent is applicable to the particular case:

- state tax authority,
- domestic and EU statistical organizations,
- courts, independent court bailiffs,
- prosecution,
- law enforcement and penitentiary organizations,
- national security services,
- a government audit organizatio controlling the regularity and expediency of using central budget funds,
- authority acting as financial information unit,
- ministries and their background institutions,
- Hungarian National Bank,
- State Audit Office of Hungary,
- European Anti-Fraud Office (OLAF),
- public notaries
- notaries,
- financial institutions, credit institutions, card issuers.

The framework for mandatory data transmission
In order to perform their mandatory duties, the above-mentioned organizations may request or receive your personal data from the Treasury for the purposes and under the conditions specified in the relevant legislation.
Data transfer without personal data
In addition to the above, your data may be transferred in a personal and confidential manner, so that you may not be in contact with the data under any circumstances (eg anonymous statistical data, anonymised data).

Period of data management

In the case of **the performance of a task in the public interest and the exercise of public power**, **and mandatory data management**, the Treasury handles your data until the deadline specified in the data management legislation.

Where the law does not set a time limit for the processing of personal data, the Treasury handles the data for the shortest period of time necessary to achieve the purpose of the data management. In order to comply with this, the Treasury shall manage the data based on Info tv according to its requirements, every three years from the commencement of data management, it shall review whether the processing of personal data managed by it or by its processor or acting on its instructions for the purpose of data management is required.

Within the framework of mandatory data management, the Treasury handles certain data related to the acquisition of rights that should be protected by a level of protection similar to that of property protection. Such treasury data will be handled by the Treasury until the claimant or the relative has the right to enforce the claim (for example the right to claim a pension insurance does not expire).

The Treasury manages the data related to the eligibility to verify the validity of the entitlement and for the period necessary to verify its legality.

In the case of **contractual data management**, the duration of the data processing shall extend to the duration of the contract, provided that the contract does not foresee further data processing for a specific legitimate purpose for a definite period of time after termination. In any case, the data is processed only for the time necessary to achieve the purpose of data management. In the event of termination of the contractual legal basis, the management and preservation of the data related to the given contract based on a legal obligation shall be preserved if the data are also subject to mandatory data management.

In the case of **data management related to the contract**, the data can be managed for the time necessary to enforce the contract or the legal claims arising therefrom (for example due to a change in the contact person, the handling of the previous contact information is no longer necessary).

In the case of **data processing based on voluntary contributions**, the duration of data management is always limited to the required amount. Detailed information given to you prior to your consent includes either the specific duration or the criteria for determining the duration.

The duration of data processing **related to the protection of persons and property and the provision of physical conditions for IT security** is determined by the legal regulations, the security regulations in force at any time, and the prospectuses annexed thereto.

Duration of mandatory data management for Treasury investment services and ancillary services:

Nature of activity	Applicable legislation	Required retention period
Investment service	Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing	8 years after the termination of the contract
Accounting documents related to investment service	Act C of 2000 on Accounting	8 years from the date of issue of the accounting document
Tax certificate related to investment service	Act CL of 2017 on the order of taxation	the right to a tax assessment is time-barred 5 years
Electronic securities distribution	Act CVIII of 2001 on certain issues of electronic commerce services and information society services	until the last invoice after the termination of the contract
Customer due diligence measure	Act LIII of 2017 on the Prevention and Combating of	1. Transaction order: 8 years from transaction

	Money Laundering and Terrorist Financing	2. In business relationship: 8 years after the termination of the contractual relationship 3. at the request of the Hungarian National Bank, the Anti-Money Laundering and Counter-Terrorism Financing Office, the investigative authority, the prosecutor's office, and the court, for the period specified in the request, but for no longer than 10 years from the termination of the business relationship or the fulfillment of the transaction order.
Complaint handling	Act XXV of 2023 on Complaints, Public Interest Disclosures, and Rules Related to Reporting Misconduct	5 years
Property protection	Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation Activities	in the absence of use, up to 60 days from the date of recording

Who can access the data which manage by the Treasury?

Employees of the Treasury
Personal data can be accessed by employees of the Treasury to perform their duties, to the extent necessary. Employee access rights are limited to their own field of expertise, so even within the Treasury, no person can access your data that is not part of his/her job.

Use of data processors
If the law or the consent given by you allows, the Treasury may entrust the processing of the data to the other data processor. Data processors must follow the same strict privacy and information security rules that the Treasury also applies to protect your data. The rules of data processing are partly contained in the legislation prescribing this activity of the Treasury and partly in the agreements concluded with the data processors.

Treasury as a data processor
In fulfilling its statutory obligations, the Treasury acts as a data processor in certain matters or during the operation of certain systems.

As a data processor, the Treasury adheres to the same strict data protection and information security requirements as data controllers, however, in such cases, detailed data management information will be provided to the data controllers for which the Treasury performs its data processing activities.

As a data processor, the Treasury will take all necessary measures to ensure that the data controller - for whom the Treasury performs data processing activities - can effectively support the exercise of your rights.

Authorized organizations
In addition to the above, only the bodies and persons authorized to know the data in the law can access your data within the scope of the law (for example police, State Audit Office of Hungary, National Archives of Hungary etc.).

Data security measures

The Treasury stores personal data electronically on servers located at its headquarters and premises, and on paper, in its archival systems, and provides appropriate IT security, technical and organizational measures to protect the personal data it manages, including unauthorized access or unauthorized alteration of data.

To this end, the Treasury has an extensive IT Security Document System which is regularly reviewed. It regulates, among other things, the access rights to the data stored in each IT system, which the Treasury logs to see who, when, what personal data it has access to control.

In its operation, the Treasury fulfills the current statutory requirements for IT security for public organizations (at present, Act L of 2013 on the Electronic Information Security of State and Local Government Organozations and the decree on 41/2015. (VII. 15.) BM).

For some of its activities, the Treasury is obliged to comply with strict international standards (for example ISO 27001), which also guarantee data security.

The security of paper-based document management is ensured by the Treasury's Document Management Rules and the Security Rules of the Treasury's buildings and physical operations.

The Treasury has a Data Protection and Data Security Policy that is regularly reviewed and is bound to appoint a Data Protection Officer to ensure the protection of your data.

What rights do you have for your managed personal data?

Right to information
You are entitled to provide from the Treasury with brief, transparent and comprehensible information on the essential aspects of data management, the rights you exercise and the remedies available immediately before the data processing is completed or at the latest after the first processing operation. In view of this right of prior information, this information has been published. It should be noted that you may have additional rights and remedies related to data management when you verify your identity.

Right to know of data ("right of access")
You are entitled to request information from the Treasury on the personal data manage about you, the purpose, legal basis, duration, legal basis and recipients of the data transfer.

Rights for correction (modification), deletion, restriction (blocking)
You have the right not only to know your personal data managed by the Treasury, but also to request the correction of your data that needs to be clarified and, in the case of non-mandatory data, to request the deletion of data and limitation of data management. [Provisions related to

data management rights and their enforcement are contained in Info Act., and GDPR.] It is not possible to request the deletion of data that is subject to mandatory statutory data management.

Right to data transfer
Upon exercising the right to data transfer at the request of the Affectedt, the Data Manager shall transmit the data which available about the Affected, in a distributed, widely used, machine-readable form, or forward it to another data manager upon request. This right can only be exercised if the data processing is based on consent or performance of a contractual obligation and the data processing is automated.

Affected has the right to use his / her right to data transfer only through a personal appearance at a customer service offices engaged in distribution of government securities, as well as in a letter or e-mail attachment. You must complete or submit the pre-completed Form at the time of your personal appearance. It is only possible to receive a letter or e-mail attachment if this form of communication has been defined as a communication channel for the Affected, and it is recorded in the Treasury's securities trading system. The Form can be applied in person to any customer service office of the Treasury, or downloadable from the Treasury's website (http://www.allamkincstar.gov.hu/en/).

Right to protest
On the base of this right, in the event of a protest, the Treasury may only process your personal data to the extent necessary for the performance of its official duties and for other mandatory data management. With regard to your not necessary data, the Treasury limits the treatment and investigates your protest. The Treasury may only process your data that is not subject to mandatory data management if it proves that the data management is justified by compelling legitimate reasons that take precedence over your interests, rights and freedoms, or which are related to the submission, validation or protection of legal claims.

If the Treasury finds that your objection is well-founded, it will terminate the processing of the data affected by the restriction and delete the data.

How can you exercise these rights?

If you have the above rights, the Treasury must inform you about the measures taken within the shortest possible time from the submission of the request, but within a maximum of twenty-five days. The information should also include which body you may turn to for the purpose of investigating your complaint regarding data management, which rights you may have to remedy your violation, and you may turn to your National Data Protection and Information Authority (NAIH) and the court for your case.

Reporting a complaint to the Treasury or NAIH
You can contact your complain about your personal data management to the Treasury (1054 Budapest, Hold utca 4, adatvedelem@allamkincstar.gov.hu) or the NAIH (1055 Budapest, Falk Miksa utca 9-11., post address: 1055 Budapest, Falk Miksa utca 9-11., Ugyfelszolgalat@naih.hu)

Judicial enforcement
If you consider that the Treasury unlawful handling of your personal data, you may initiate a civil lawsuit against the Treasury, it is governed by the jurisdiction of the court. The lawsuit can be initiated at your own discretion before the competent court of your living place or place of residence (see the list of judges and contact information via the following address: https://birosag.hu/en).

Effective from: 8th January 2024.