Case number: NAIH / 2019/3107/7.

Subject: Decision

DECISION

Before the National Data Protection and Freedom of Information Authority (hereinafter: the Authority), Raiffeisen Bank Zrt. (Registered office: 1054 Budapest, Akadémia utca 6 .; tax number: 10198014-4-44., The hereinafter 'the Bank') initiated ex officio data protection proceedings against Authority examined the Bank's general data management practices related to MiFID questionnaires, a Authority shall take the following decisions:

I. Notes that the Bank

(1) handles premium and private only non-advisory services without a legal basis personal information provided by customers in the aptitude test;

(2) does not provide adequate information on personal data included in MiFID questionnaires management.

II. Instructs the Bank to do so within 60 days of the date on which this resolution becomes final

(1) delete the personal data of premium and private customers provided in the aptitude test, who do not use the Bank for investment advice or portfolio management service;

(2) adapt its disclosure practices to comply with Articles 12 and 13 of the GDPR. requirements of Articles

III. Due to the unlawful data processing, the Bank shall be notified of the 30 within a day HUF 25,000,000, ie HUF twenty-five million data protection fine obliges to pay.

ARC. It shall order the resolution to be made public by publishing the identification data of the Bank bringing.

***

The fine is a HUF settlement account for the collection of centralized revenues of the Authority

(10032000-01040425-00000000 Centralized direct debit account IBAN: HU83 1003 2000 0104

0425 0000 0000). When transferring the amount, NAIH / 2019/3107. JUDGE. for

should be referred to.

If the Bank fails to meet its obligation to pay the fine on time, a late payment surcharge

is obliged to pay. The amount of the late payment allowance is the statutory interest affected by the delay

equal to the central bank base rate valid on the first day of the calendar half-year.

2

A II. obligation under point III. The fine and the late payment allowance shall not apply

the Authority shall order the enforcement of the decision.

Until the expiry of the time limit for bringing an action against the decision, or an administrative action

until the final decision of the court, the data involved in the disputed data processing shall not

may be deleted or not destroyed.

A II. within 8 days of the measures provided for in paragraph 1

- together with the supporting evidence, shall notify the Authority. To the Bank

as evidence, fully document the fact of the deletions and the IT circumstances

protocol (s) and a statement that the named data / databases

all copies have been deleted.

There is no administrative remedy against this decision, but from the date of notification

within 30 days of the action brought before the Metropolitan Court in an administrative action

can be challenged. The application must be submitted to the Authority, electronically, which is the case

forward it to the court together with his documents. The request for a hearing must be indicated in the application. THE

for those who do not benefit from full personal exemption, the judicial review procedure

its fee is HUF 30,000, the lawsuit is subject to the right to record material fees. In the proceedings before the Metropolitan

Court a

legal representation is mandatory.

EXPLANATORY STATEMENT

I. Procedure and clarification of the facts

(1)

On 28 November 2018, the Authority initiated an ex officio investigation with the Bank's MiFID questionnaires

to examine its general data management practices in relation to NAIH / 2018/6739 / V.

case number. The Authority closed the ex officio investigation procedure on 26 March 2019 and

at the same time, the Bank initiated ex officio data protection official proceedings against the investment

compliance and suitability tests applied in the course of its service activities (a

hereinafter referred to collectively as the MiFID Test or MiFID Questionnaire)

the General Data Protection Regulation (hereinafter: GDPR)

to verify compliance with the requirements. The Authority is the present data protection authority

In the course of the proceedings, the Bank took into account NAIH / 2018/6739 / V. in its proceedings

is.

(2)

The investigation period is 25 May 2018 to the date of initiation of the proceeding, 26 March 2019

tart.

(3)

In its reply dated 15 December 2018 (NAIH / 2018/6739/3 / V.), The Bank stated that

that it does not carry out cross-border activities in connection with the data management activities under investigation

data management. He confirmed this statement in his reply of 31 May 2019,

according to which the Bank is the data controller in connection with the examined data management, so it brings the

decisions on the purpose, legal basis and legal compliance of data processing.

(4)

The Bank has informed the Authority that MiFID II has entered into force on 3 January 2018

Regulation - Directive 2014/65 / EU of the European Parliament and of the Council on financial instruments

markets and amending Directive 2002/92 / EC and Directive 2011/61 / EU

into the Hungarian legal system about investment companies and commodity exchange service providers,

and Act CXXXVII of 2007 on the rules of the activities they may carry out. law

(hereinafter: Bszt.). Due to strict investor protection rules a

banking group has changed its previous practice and investment services

made it mandatory for the use of the Bszt. Compliance pursuant to Section 45 (1)

test completion.

3

(5)

In the compliance test, the Bank assesses the services, services and services known to the customer

financial instruments, examines the characteristics of the client's previous transactions,

examine whether the client has relevant financial knowledge or expertise

experience, in order to really make the right deal or financial for him

provide a service related to the device.

(6)

The Bszt. The Bank shall only make the completion of the aptitude test pursuant to Section 44 mandatory

for its customers or prospective customers (collectively, the Customer), if any

enter into an agreement with the Bank, on the basis of which they become entitled to investment advice

or to use a portfolio management service.

(7)

The Bank assesses the client's investment objectives and risk-bearing in the suitability test

willingness, financial standing, loss - making capacity and experience and

knowledge of the nature of services and products, including related

ability to understand and assess risks.

(8)

The Bank is the first to enter into a framework agreement with its customers for the provision of investment services. THE

may request any of the services covered by the framework contract

with the client's unilateral disclaimer. For the use of this service

the client may make his statement in writing and through a fixed line oral channel.

(9)

Upon concluding the framework agreement, the customer shall contact the Bank in person,

Thus, information handouts requiring personal consultation and presence will be handed over at this time,

making legal statements and completing questionnaires, including MiFID tests. From this

resulting from any legal relationship governed by the framework contract

to fulfill an obligation which cannot be performed later or to do so

possibly impossible due to circumstances later, this should happen.

(10) The compliance and suitability test is part of the framework contract as they are required

a legal obligation relating to certain legal relationships covered by the framework contract

to fulfill.

(11) The Bank has not provided so-called […] services since […], only […] and […] services.

This was decided at the […] meeting and is included in the customer rating as well as the

No. […] on guidelines for investor-based and investment-based advice

CEO instruction B.2.2.1.1. also point.

(12) During the execution-only service, the Bszt. Section 5 (1) a) and b)

specific services, - taking and transmitting an order, or

execution of an order for the benefit of the customer - the subject of which is not a complex product.

(13) As part of a non-advisory service, the Bank provides its customers with the product it offers

information on possible investment alternatives

without expressly recommending a specific product to the customer. THE

Bank discusses the main advantages, disadvantages and risks of possible investment alternatives,

informs the customer about the fees and commissions, provides general information about the products,

presents the full product range from which the customer selects the product they want to buy

and decides on the granting of the order on the part of the Bank regarding the conclusion of a specific transaction

proposal cannot be made.

(14) The Advisory Service provides a narrower analysis of different types of assets

taking into account the client's risk-bearing capacity. During investment advice

typically personalized recommendations for specific products are made.

4

(15) An advisory transaction is entered into if the client is recommended by the Bank after the advice

decides to enter into a specific transaction. Non-advisory transactions are those

transactions where, following advice from the advisory service, the

the client requests the execution of a transaction other than the one recommended in the course of consulting, or

as part of a non-advisory service requested by the client following general advice

execution of a transaction.

(16) The Bank divides its retail clients using investment services into three groups:

mass, premium and private categories. To change the customer category, the customer

at any time of his choice - and subject to certain property and income conditions

may take place by terminating the existing legal relationship and applying to the new legal relationship

by concluding a contract.

(17) The Bank does not provide investment advice or advice to the mass client group

portfolio management service, so it is not filled in with clients belonging to this client group

the aptitude, only the compliance test.

(18) The Bank's choice of the customer in case of certain income or property conditions

contract for premium or private banking customer service

service. Customers in these categories will benefit from the mass

compared to this category, they receive different discounts, such as more personal

service - they have their own contact person - the possibility to use counseling. THE

There are also significant differences between the two segments in terms of the range of products available: a

The range of investment funds is wider for clients belonging to the private segment, the

scale of advisory investments, the Bank provides them with the opportunity to telephone

financial planning, investment advice or engagement

in addition, they may use a portfolio management service available

for them, the pawnshop, the Platinum credit card, and other amenities and accessories

they receive services, including the possibility outside the bank branch

for trial.

(19) The Bank is available to both premium and private customers

provides investment services with and without investment advisory, however

not exclusively for the provision of non-advisory services to clients in this category

concludes a contract because when concluding a framework contract for investment services

they will automatically have access to the advisory service. The

in the absence of an aptitude test, investment advice to clients; or

portfolio management service cannot be provided. Investment advice is part of everyday life

customer negotiations, so that the Bank can provide its private and premium customers with a

provide the right service for their segment - that is, investment advice at any time

it is justified to complete the aptitude test at the time of concluding the contract. From this

therefore, the Bank considers the suitability test necessary for these two customer groups

completion. This is because the Bank considers it unrealistic for the customer then

you have to get tired of a bank branch to complete the aptitude test when you already have

you want to use an investment advisory or portfolio management service.

(20) The Bank allows MiFID tests to be completed on a website provided by the Bank's rapporteur a

can be accessed from the Bank's system on the basis of the completed questionnaire identification number.

(21) On 31 May 2018 […] private and […] premium, on 28 December 2018 […]

was a private and […] premium customer. Between January 3, 2018 and July 26, 2019 […] private

and […] premium client has not entered into an advisory transaction. In this number, those customers

for whom the Bank provides investment advisory services,

however, the customer did not request the execution of a specific transaction recommended by the Bank.

5

The purpose of the processing of personal data included in aptitude and compliance tests is to:

the Bank should be able to protect investors during transactions

provide information and feedback to the client on how well the given transaction fits

the risk-bearing, load-bearing capacity and knowledge of the product

how sufficient they are to complete the transaction. Another goal of the Bank is legal

including the obligation to investigate the target market and supervisory requirements

- MNB, ESMA recommendations that protect investors, prudent financial institutions

and be able to meet the requirements of your group.

(23) The obligation to carry out a target market test is laid down in Bszt. 17 / A. § and Bszt. § 40

Paragraphs 2 to 3 shall apply to the Bank.

(24) The complex nature of the processing of personal data recorded in MiFID questionnaires

In view of its different purposes and the differences in the legal basis arising from the regulations, the Bank has several

with reference to the legal basis in the customer compliance and suitability test

provided. The legal basis for data management is partly the legal obligation of the Bank

fulfilling the legitimate interest of the Bank, partly with the customers

performance of the contract. An interest balancing test to prove the Bank's legitimate interest

submitted to the Authority.

(25) When completing the MiFID test in person, the Bank's rapporteur shall orally inform the client a

A brief overview of the essence and purpose of the MiFID test, as well as on the form itself

information. When completing the MiFID test on the website, the Bank provides information on the website.

In connection with the handling of personal data recorded in MiFID tests, the Bank is available on its website

provides information in the Privacy and Data Management Information

in the MiFID Prospectus specifically for data protection purposes. Specifically for MiFID

no separate information on the handling of personal data provided in the tests

as it considers that it has no legal obligation to do so.

(26) The Bank shall make the investment facility available to the client prior to the conclusion of the contract

the terms and conditions announced in connection with the services, which are provided by the Bank

also available on the website. Provision of investment services and ancillary services

The Bank shall clearly inform the customers in the framework agreement on

customers acknowledge by signing the framework contract that the prior notice required by law

information is provided by the Bank on its website. To the Bank as an investment company

provide timely information to its customers in order to ensure that

customers should have sufficient time to understand the information and make informed decisions

to take. Sectoral legislation on the provision of investment services does not

require investment firms to make sure that Clients

they were indeed familiar with the content of the information.

(27) In addition, the Bank has implemented MiFID II. brought changes to the contracted customers in a letter

notified in December 2017, which is also available on the Bank's website. This information

The letter also stated that the renewable MiFID test was suitable for the Bank to conduct the

target market investigation.

II. Applicable legal provisions

Pursuant to Article 2 (1) of the GDPR, the processing of data in the present case requires the GDPR

apply.

The relevant provisions of the GDPR in the present case are the following:

GDPR Article 6 (1) (a), (b), (c), (f) and (3): Personal data

is lawful only if and to the extent that it is at least one of the following

fulfilled:

(a) the data subject has given his or her consent to the processing of his or her personal data for one or more specific

purposes

treatment;

(b) processing is necessary for the performance of a contract to which the data subject is party

at the request of the party concerned or before the conclusion of the contract

necessary to do so;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(f) processing for the legitimate interests of the controller or of a third party

necessary, unless those interests take precedence over such interests

interests or fundamental rights and freedoms that protect personal data

especially if the child concerned.

3. The legal basis for the processing referred to in points (c) and (e) of paragraph 1 shall be the following

state:

(a) Union law, or

(b) the law of the Member State to which the controller is subject.

The purpose of the processing shall be determined by reference to this legal basis and in accordance with paragraph 1 (e).

It must be necessary for the processing referred to in

in the public interest or in the exercise of a public authority conferred on the controller

to perform a task. This legal basis may include the provisions of this Regulation

provisions adjusting the application of the rules, including the processing of data by the controller

the general conditions governing the lawfulness of the data, the data which are the subject of the data processing

the data subjects, the data subjects, the legal entities with which the personal data may be disclosed,

or the purposes of such communication, the restrictions on the purpose of the processing, the

the duration of data storage and data management operations, as well as other data management

procedures so as to ensure lawful and fair data management

measures, including Annex IX. other specific data management as defined in Chapter

situations. Union or Member State law must pursue an objective in the public interest, and

it must be proportionate to the legitimate aim pursued.

GDPR Article 12 (1): The controller shall take appropriate measures to that end

in order to provide the data subject with the processing of personal data in accordance with Articles 13 and 13

All the information referred to in Article 14 and Articles 15 to 22. and Article 34

information in a concise, transparent, comprehensible and easily accessible form, in a clear and concise manner

provide, in plain language, any address addressed to children

for information. The information shall be provided in writing or otherwise, including, as appropriate

electronic means must also be provided. Oral information may be provided at the request of the data subject,

provided that the identity of the data subject has been otherwise established.

GDPR Article 13 (1) - (2): If the personal data of the data subject are

collected from the data subject, the controller shall, at the time of obtaining the personal data,

provide the data subject with all of the following information:

(a) the identity of the controller and, if any, of the controller 's representative; and

contact details;

(b) the contact details of the Data Protection Officer, if any;

(c) the purpose of the intended processing of the personal data and the legal basis for the processing;

(d) in the case of processing based on Article 6 (1) (f), the controller or

legitimate interests of third parties;

(e) where applicable, the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller is in a third country or internationally

personal data to the organization and the Commission

the existence or non-existence of a decision on compliance, or in Article 46, Article 47 or

in the case of the transmission referred to in the second subparagraph of Article 49 (1), a

to indicate appropriate and suitable guarantees and to obtain a copy thereof

reference to the methods used or their availability.

2. In addition to the information referred to in paragraph 1, the controller shall process personal data

at the time of acquisition, in order to ensure fair and transparent

provide the data subject with the following additional information:

(a) the period for which the personal data will be stored or, failing that, the

aspects of determining the duration;

(b) the data subject's right to request from the controller the personal data concerning him or her

access to, rectification, erasure or restriction of the processing of data, and

may object to the processing of such personal data as well as to the data subject

the right to data portability;

(c) information based on Article 6 (1) (a) or Article 9 (2) (a);

the right to withdraw consent at any time in the event of data processing,

which is without prejudice to the processing carried out on the basis of the consent prior to the withdrawal

legitimacy;

(d) the right to lodge a complaint with the supervisory authority;

(e) whether the provision of personal data is legal or contractual

whether it is based on an obligation or a precondition for concluding a contract and whether the person concerned

whether it is obliged to provide personal data and how possible

they may have consequences for non-reporting;

(f) the fact of automated decision-making referred to in Article 22 (1) and (4), including:

profiling and, at least in these cases, the logic used

understandable information on the significance of such data processing and the

the expected consequences for the data subject.

Article 58 (2) (b), (d) and (i) GDPR: The supervisory authority is corrective

acting under the authority of:

(b) reprimands the controller or the processor if he or she is acting in a data-processing capacity

has infringed the provisions of this Regulation;

(d) instruct the controller or processor to carry out its data processing operations

bring this Regulation into line with the provisions of this Regulation

with its provisions;

(i) impose an administrative fine in accordance with Article 83, depending on the circumstances of the case

in addition to or instead of the measures referred to in this paragraph;

Article 83 (1) to (2) and (5) (a) to (b) of the GDPR: 1. Each supervisory authority

ensure that any infringement of this Regulation referred to in paragraphs 4, 5 and 6 is in accordance with this Article

The administrative fines imposed pursuant to this Regulation shall be effective, proportionate and dissuasive in each case

be dissuasive.

2. Administrative fines shall be imposed in accordance with Article 58 (2), depending on the circumstances of the case.

shall be imposed in addition to or instead of the measures referred to in points (a) to (h) and (j) of

In deciding whether it is necessary to impose an administrative fine, or a

the amount of the administrative fine in each case

the following must be taken into account:

(a) the nature, gravity and duration of the infringement, taking into account the nature of the infringement in question

the nature, scope or purpose of the processing and the number of data subjects affected by the breach

and the extent of the damage they have suffered;

(b) the intentional or negligent nature of the infringement;

(c) the damage suffered by the data subject by the controller or the processor

any measures taken to alleviate

(d) the extent of the responsibility of the controller or processor, taking into account its responsibilities

the technical and organizational measures taken pursuant to Articles 25 and 32;

(e) relevant infringements previously committed by the controller or processor;

(f) with the supervisory authority, remedy the breach and the breach may be negative

the degree of cooperation to mitigate its effects;

(g) the categories of personal data concerned by the breach;

(h) the manner in which the supervisory authority became aware of the infringement, in particular

whether the breach has been reported by the controller or processor and, if so,

in what detail;

(i) if previously against the controller or processor concerned, in the same

have ordered one of the measures referred to in Article 58 (2),

compliance with the measures in question;

(j) whether the controller or processor has complied with Article 40

approved codes of conduct or an approved certification in accordance with Article 42

mechanisms; and

(k) other aggravating or mitigating factors relevant to the circumstances of the case,

for example, the financial gain obtained as a direct or indirect consequence of the infringement

or avoided loss.

5. Infringements of the following provisions, in accordance with paragraph 2, shall be imposed no later than 20

An administrative fine of EUR 000 000 or, in the case of undertakings, the previous

an amount not exceeding 4% of its total annual worldwide turnover for the financial year,

with the higher of the two:

(a) the principles of data processing, including the conditions for consent, in accordance with Articles 5, 6, 7 and 9;

appropriately;

(b) the rights of data subjects under Articles 12 to 22. in accordance with Article

Infotv. Pursuant to Section 2 (2), the general data protection decree is indicated therein

shall apply with the additions provided for in

Infotv. The right to the protection of personal data pursuant to Section 60 (1)

In order to enforce this, the Authority may initiate ex officio data protection proceedings. The

CL of the General Administrative Procedure Act 2016 on the data protection authority procedure.

(hereinafter: Ákr.) shall be applied in accordance with the provisions of the Infotv

additions and derogations under the General Data Protection Regulation.

Infotv. Section 61 (2) (a): The Authority may order the decision of the data controller,

or by publishing the identity of the processor

if the decision affects a wide range of persons.

Infotv. Section 61 (6): Deadline for bringing an action open to challenge the decision

or until the final decision of the court in case of initiation of an administrative lawsuit

data affected by data processing may not be erased or destroyed.

Infotv. 75 / A. § according to Article 83 (2) - (6) of the General Data Protection Regulation

exercise the powers set out in paragraph 1 in accordance with the principle of proportionality,

in particular by providing for the law or regulation on the processing of personal data

Requirements laid down in a binding act of the European Union

to remedy the breach - Article 58 of the General Data Protection Regulation.

in particular by alerting the controller or processor

to take action.

Bszt. Section 5 (1): Regular investment services are considered to be investment services

in the context of an economic activity for a financial instrument

a) receiving and transmitting an order,

b) execution of an order for the benefit of the client,

c) own account trading,

d) portfolio management,

e) investment advice,

(f) the placement of a financial instrument to receive an asset (security or other financial instrument)

commitment (underwriting guarantee),

(g) the placement of a financial asset in connection with the purchase of the asset (financial asset)

without commitment, and

h) operation of a multilateral trading facility,

(i) the operation of an organized trading facility.

Bszt. 17 / A. § (1) - (2): Financial for the purpose of sale to customers

an investment firm that approves individual financial instruments; and

the process for approving major adjustments to existing financial instruments (a

hereinafter referred to as the product approval process)

review before placing or distributing a financial instrument to clients.

(2) The product approval process shall identify the identified target market for final customers

within each client category of financial instruments and ensures that that particular is identified

all relevant risks to the target market are assessed and planned

distribution strategy is in line with the identified target market.

Bszt. Section 44 (1), (2): An investment firm that provides investment advice

or perform a portfolio management activity in the framework of that activity in paragraph 2

the conclusion of the contract or, in the case of a framework contract, the contract

prior to its implementation

(a) satisfy himself that the prospective contractor and the client know the contract and the contract

or its practice in relation to the financial instrument or transaction that is the subject of the mandate,

whether its risk-bearing capacity is adequate to make an informed investment decision

bring and

(b) disclose to the extent necessary for the performance of the contract

the income position and investment objectives of the counterparty or the client,

in order to adapt to its circumstances with its ability to bear losses

and suitable for meeting your investment expectations; or

recommend a financial instrument.

2. The information specified in paragraph 1 (hereinafter referred to as the aptitude test)

the investment firm evaluates its investment advisory activities or

Commission (EU) 2017/565

as set out in Articles 54 and 55 of the Delegated Regulation

compliance.

Bszt. Section 45 (1): An investment firm that is not in Section 44 (1)

the investment service activity referred to in paragraph 1, the conclusion of the contract or

in the case of a framework contract, before the execution of the contract, in paragraph 3

with a specified exception, request a statement from the prospective contractor and the client

a) the substance of the transaction included in the contract,

10

(b) the characteristics of the financial instrument involved in the transaction; and

(c) in particular their risks

knowledge and experience of the investment firm in order to assess whether the investment

the undertaking is indeed involved in a transaction or financial instrument that is appropriate to it

provide a service.

2. The assessment of the knowledge and experience referred to in paragraph 1 (hereinafter:

compliance test), the investment firm shall comply with Commission (EU) 2017/565

as set out in Articles 55 and 56 of the Delegated Regulation

el.

Bszt. Section 46 (1): If the investment firm is covered by Section 45 (1)

on the basis of certain information, considers that the financial

asset or transaction is not suitable for the prospective counterparty or client to do so

draws the attention of the prospective contractor or the client.

(2) If the prospective contracting party or the client does not specify in Section 45 (1)

specified information or the information provided by the investment firm

considers it insufficient, draws the attention of the prospective contractor or the client to the fact that

in this case, the financial instrument or transaction included in the contract is incapable

to determine its adequacy.

3. The warning provided for in paragraphs 1 and 2 may be issued in a standardized format.

III. Decision:

III.1. Legal basis for data management

III.1.1. Fulfillment of a legal obligation

(28) According to the Bank's statement, the personal data included in the MiFID questionnaires are partly legal

under its obligation.

(29) The obligation to use MiFID tests is laid down in Bszt. transposed it into Hungarian law. The Bszt. 44.

§ (1), the investment firm is required to complete the suitability test in

with its client if it provides investment advice or portfolio management.

(30) The Bszt. Section 45 (1) provides that the investment firm must

complete the compliance test with your clients, if any, from investment advice and

provides a different service to its clients than portfolio management. The Bszt. a Section 45 (3)

It also allows exceptions to the completion of the compliance test.

(31) The Bank completes the compliance test with all its customers, as it does not provide the Bszt. Section 45 (3)

execution only service to its customers. Therefore

with all clients using investment services,

premium or private - completes the compliance test required by Article 6 of the GDPR.

legal obligation under Article 1 (1).

(32) The handling of personal data provided in the aptitude test is a legal obligation of the Bank a

Bszt. § 44 (1) if investment advice or portfolio management

provides a service to its customer. Providing investment advice or portfolio management

however, in the absence of such processing, the processing of personal data provided in the aptitude test will no longer take

place

the legal obligation of the Bank, so its premium and private customers are specified in the suitability test

the Bank manages its data on the basis of its legitimate interest.

III.1.2. Data management based on the legitimate interests of the Bank

(33) According to the Bank, non-advisory premium or

The personal data provided by private customers in the suitability test is valid by the Bank

in the interests of the Member State.

(34) In relation to the processing of data by reference to the exercise of this legitimate interest, the Authority

highlights that client rating as well as investor-based and investment-based advice

CEO's instruction […] on its policies B.3.1. According to point a

clients who do not use investment advisory and portfolio management services

only requires you to complete the compliance test. The above CEO instruction is not

delimit which customer needs compliance and which customer eligibility

and also complete a compliance test to be classified as mass, premium or private,

but what kind of service you use.

(35) The Bank carried out a balancing of interests in support of its legitimate interest, which

submitted to the Authority a balancing test. The

deliberation test dated January 2, 2019. The Applicant submitted the application on 25 May 2018 and 2019.

has not submitted a balancing test for a legitimate interest for the period from 2 January

to support it.

(36) The Authority will further examine the Bank 's handling of data on the basis of a legitimate interest, namely:

whether the Bank has a legitimate interest or whether data management is necessary for its enforcement,

and whether the legitimate interest of the Bank over the interests of the persons concerned actually takes precedence,

fundamental rights and freedoms.

(37) In the interest test, the Bank has three purposes for its data management based on its legitimate interests

which can also be understood as a legitimate interest which it has identified, in particular because

Bank has never explicitly named the legitimate interest to enforce

considers data management necessary.

Fulfillment of a legal obligation as a legitimate interest

(38) According to the balancing test, the purpose of the Bank 's data management based on a legitimate interest is to:

compliance with legislation, HFSA, MNB and ESMA recommendations, investors / clients

protection and prudent operation.

(39) The specific legal requirements with which the Bank has a legitimate interest

considers the following: Bszt. 44-46. § on compliance and suitability tests

legal provisions requiring prior information through

and the Bszt. 17 / A. § provisions requiring the definition of the target market.

(40) During compliance with the resolutions, the Bank is the MNB and the European Securities Market

It is understood to comply with the recommendations of the Authority (ESMA). The Bank has a legitimate interest

10/2019. (IV.15.) And 25/2018. (VII.5.)

recommendations and the requirements of ESMA35-43-620 and ESMA35-43-1163

wants to meet. For product approval requirements governing capital markets

issued in connection with 25/2018. (VII.5.) Of the MNB, the MNB shall ensure that the

ESMA35-43-620. on MiFID II for product management

compliance with the guidelines, while governing the provision of investment services

on certain aspects of the proper fulfillment of the obligation to provide prior information

10/2019. (IV.15.) Of the MNB, ESMA35-43-1163, MiFID II

guidelines on certain aspects of eligibility requirements under

ensures compliance. So the Bank referred to two MNB and two ESMA recommendation pairs

adjustable, their content is essentially the same. The Bank did not specify exactly that

you consider the advisory service necessary to comply with which parts of the recommendations

specified in the suitability test by premium or private customers who do not use it

processing of personal data.

(41) The Authority considers it necessary to state that recommendations do not constitute legislation,

they may not create a legal obligation.

(42) The Bszt. 44-46. § does not require the Bank to complete it in that case either
the suitability test with the customer if the customer does not use a service that
for which the data contained in the aptitude test are required. The Bszt. is
provides in Section 44 (1) that investment advice or portfolio management
prior to the execution of the mandate for this service
you have to make sure in the suitability test your client Bszt. Section 44 (1) a) and b)
about your knowledge, circumstances and preferences. So the fitness
prior to completing the test, the Customer must initiate the provision of the Bank by the Customer
provide investment advice or portfolio management. The Bszt. Section 45 a
compliance test, which is required by all of the Bank's legal obligations
with the client, while the Bszt. Section 46 regulates the procedure to be followed a
To the Bank if, on the basis of the compliance test, the financial instrument or transaction included in the contract
is not appropriate for the customer, or the customer does not complete or does not complete the
compliance test. It does not follow from these legal provisions that
according to which the Bank should also deal with customers who do not use the advisory service
pass the aptitude test, which is also recognized by the Bank itself in the balancing test
in its introduction, according to which "even without an explicit legal obligation, it completes a
compliance test and aptitude test '.

(43) The Bszt. 17 / A. § requires investment firms, including the Bank, to maintain and operate a product approval process.
The product approval process
as a result, the target market for a product is defined, ie in which category
belonging to (retail / professional client or eligible partner), what preference is given to clients
the product (ideal target market) may be ideal for them and what are the customer groups
for whom it is not recommended at all (negative target market). Neither the Bszt. Nor the Bank
otherwise not relied on by the investment firm in the balancing test

16/2017 on the applicable product approval process (VI. 30.) NGM decree no

define the method for defining the target market, for which guidance ESMA3543-620 provides guidance. A 10/2019. (IV.15.)

Cannot be taken into account

that it was issued by the MNB on 15 April 2019 and its application from 15 May 2019

expects from the financial institutions concerned, while in the present data protection authority proceedings a

end of the period under review March 26, 2019

(44) The Bank has performed the balancing test II.1. points out that premium and private customers

the processing of personal data included in the aptitude test is necessary to reach the target market

fulfill the obligation to carry out an inspection. In his view, if the data management

would be unable to fulfill its legal obligation.

(45) Where a processing operation is necessary for the controller to comply with the law

comply with its obligations and comply with the legal requirements applicable to it,

The legal basis for the processing of personal data is the legal basis under Article 6 (1) (c) GDPR

obligation. The legitimate interest of the controller may only be an interest which is not

arises from a legal or contractual obligation, as in these cases the

data processing is not an enforcement of a legitimate interest but a legal obligation or contract

to fulfill its obligations.

13

(46) The Bank did not define what it meant by target market investigation: the product approval process,

as a result of which it determines the target market of the product or the control of the target market, i.e.

examining whether the customer falls for the negative or positive of that product

the target market for which you wish to place an order. V-6/2018 on the principles of product management.

CEO's instruction no. uses the concept of target market research, instead target market

talks about definition and target market control. Consequently, it cannot be identified that a

Exactly which obligation the bank would not be able to fulfill in the absence of data management.

(47) The Bank did not explain or justify why it would not be able to meet the target market

why it would not be able to determine what it produces and markets

target market for products or control the target market if premium or private

would not fill in the category of non - advisory clients

aptitude test.

(48) The Bank is only a distributor for certain products and a producer and producer for other products

distributor. In both cases, there is an obligation to define the target market. Recommendation 34-37 of ESMA35-43620. The

actual target market must be defined as the distributor in accordance with

the type of customer to be taken into account should be taken into account when defining the target market

provides investment services, so make your decision on, among other things, your own client base

should be based on existing information and knowledge You need to use it for this

all reasonably useful and accessible information and data available to it,

or which can be collected through investment and ancillary services.

(49) However, it does not follow from ESMA Recommendation 35-43-620 above that a

A bank would be required to collect data from its customers that is not explicitly

necessary to provide the service of choice to the customer and the

to fulfill the legal obligations relating to the service. The recommendations

in no case may they override the legal provisions and their interpretation

it may not lead to a result that is contrary to law or not

can be deduced.

(50) Section B.4 of the […] CEO's instruction. provides that at the points of sale to the Bank

you must have a process that allows the customer to make a unique request

may be verified before the transaction is entered into for that financial instrument or

Positive - and possibly negative - Target Market and Distribution for this product group

Against strategy. This process is nothing more than checking the target market. The CEOs

according to the instruction, depending on the type of investment service provided to the client (advisory or nonadvisory), the

minimum amount of data that the Bank must verify. Where the customer

intends to use a service that does not involve investment advice, the Bank will only use it

you need to check that the client who wants to give the order is a retail, professional client or

acceptable partner and what knowledge and experience you have

(as stated by the customer in the compliance test). It is required by the CEO's instruction

and also to provide non-advisory service to clients in advance

be warned that there may be limited target market monitoring where advice is provided

in the case of transactions carried out in the context of a wireless service.

(51) This also means that the monitoring of the target market is not hindered by the

if the premium or private customer does not pass the suitability test,

as it is limited but can be done as the Bank does for compliance only

also for mass clients in the test.

(52) Based on the above, the legal provisions and recommendations referred to by the Bank are in themselves

they do not impose on the Bank any legal obligation to fulfill them

by premium and private clients using only non-advisory services

handling of personal data provided in aptitude tests. In addition, the Bank

has not been substantiated by any additional legal provisions and recommendations referred to

legitimate interest that would require the data processing in question to be enforced.

Protecting investors and customers as a legitimate interest

(53) The Bank considers that the non - advisory premium and

handles personal information provided by private customers in the aptitude test for that purpose

also "to provide to its customers only and exclusively

which are in line with the specific needs of the particular customer and potential load bearing capacity

thereby increasing transparency and confidence

investment services and the Bank. "

(54) In the Bank's view, the non-advisory premium or

you can protect it by handling the data you provide in the aptitude test

customers from entering into transactions that are not in accordance with

their willingness to bear the risk, and thus their financial position, loss-making

their ability to recommend the product that best suits their needs.

(55) In the Bank's view, it would 'cause very serious disadvantages' to those concerned

non-management of data, as the Bank provided the data provided in the suitability tests

would not provide the security that investment services can expect

in the case of recourse to In the absence of data management, customers would not have

information on each transaction to be concluded, so that customers are certain

segment would be much more exposed to individual investment risks.

(56) In the Authority's view, the Bank did not carry out a balancing test

finding that in the absence of completing the aptitude test, customers do not

have sufficient information on each transaction to be concluded, as the Bank

states that it also provides general information on non-advisory transactions

customers about the transactions they have chosen and their possible alternatives,

which information service is independent of whether the client has completed the eligibility

test because the mass customer group only provides such a service.

(57) In addition, the […] CEO's instruction to the Bank on product management principles

B.4. It is not only the customer data that is required when monitoring the target market

take into account the target market and distribution of the product

strategy that sets out the type of customer for the product (retail, retail).

professional client or eligible partner), through which distribution channel (execution only, nonadvisory, advisory), to which

category of clients it may be sold. If a premium

or a private client uses only a non-advisory service, so does not request

investment advice, only a product that is the target market can be sold to him

can be marketed as a non-advisory service by definition, so it cannot be concluded

a transaction for a product that is only available as part of an advisory service.

(58) The Authority does not dispute that if customers complete the aptitude test, there will be more
data will be available to the Bank on its customers, including their financial position,
their loss - making capacity, their investment objectives, the duration of the investment,
personal data about their risk appetite. Possession of this data
the target market check and the Bank's customer can be performed more accurately and completely
provide information on the most suitable products for you. Given that investor protection

the purpose of the measures is to protect customers from entering into transactions that are not suitable for them,
therefore, it is not primarily in the interests of the Bank but in the interests of its customers.

(59) Legislation determines the level of protection that investment service providers,
Thus, the Bank must also ensure that it protects its customers. For the Bank
an overarching, paternalistic decision to get the level of protection required by law
provides a higher level of protection for non-advisory services only
buyer for premium or private customers. The Bank neither in the interest balance test nor in the
in its statements, it did not explain why it differentiates between the same services
among mass, premium and private customers, we justify the latter two categories
enhanced protection for customers - and a personal aptitude test
the need to process their data.

(60) The above does not mean that the Bank cannot provide higher than required by law
a level of protection that requires the processing of additional data not required by law,
however, it should also be noted that in itself is a data processing concerned
does not legitimize the processing.

(61) In the Authority’s view, it should be left to the discretion of customers whether they wish to
to enjoy a higher level of protection than that provided for by law, or
no. If so, premium and private customers can choose to complete the

aptitude test even if they do not otherwise use a service a

Bank, which would make it necessary, thus ensuring their right to information self-determination

enforcement.

(62) In the interest test, the Bank did not consider as an alternative that customers

whether data may be processed with the consent of customers in order to protect their interests,

which are used by premium and private clients using only non-advisory services

are given in the aptitude test, although data processing on the basis of consent - if a

all requirements for consent are met - less intrusive for the private sector,

as mandatory data management based on the legitimate interest of the Bank.

Prudent operation of the Bank as a legitimate interest

(63) According to the balancing test, the Bank 'will pay particular attention to

also to comply as fully as possible with the law in all cases,

and the expectations of the legislature behind them. And within that framework

in some cases even without an explicit legal obligation, in the interests of investors

seeks to incorporate protection mechanisms into its operation that

promotes a responsible, prudent operation. "

(64) The Bank stated that it would not be able to meet the internal standards set by its group

prudential requirements and would not be able to provide its own investment services in such a way

provided in a way that meets your own security expectations, if not

would treat the non-advisory private and premium categories only

personal data of your customers in the aptitude test. If the Bank did not do

data protection would be less protective of the interests of its own customers and thus less

public confidence would also be greatly reduced.

(65) Prudential requirements set by the Bank's group of companies and the Bank's internal

compliance with its security requirements are all abstract, general, imprecisely defined

interests and goals. The balancing test did not explain clearly and in detail

what the Bank means by internal security requirements or prudence requirements, which

although it also means that it is not transparent and clear to the parties concerned that the Bank is in charge of this

whether its interests in meeting those expectations actually override its right to

have control over their personal data themselves.

(66) In the Authority's view, if the Bank is subject to investor protection in the Bszt

intends to ensure a higher level of protection for its customers than the requirements of

it may be an appreciable interest, but it must specify what you intend to provide

the level of security, how and how it can be achieved and demonstrate that

how and in what way data management serves this interest. The Bank is

in the necessity part of the balancing test, it was not substantiated that the data management

necessary to ensure prudent operation and why data management can be ensured

continuing to operate more prudently than in the absence of data management.

(67) The Bank considers that it passes the aptitude test for all premium and private

not only serves the interests of the customers and the Bank, but also the public

It also has significant and significant benefits for investors, as stronger investor protection is not limited to

Bank's current but also potential future customers and other participants in the financial markets

may also be particularly beneficial to “Public” and “financial markets are other

"actors" is a very broad, difficult-to-understand and unbounded definition of the scope

who may benefit from the fact that the Bank continues to process the data under review.

(68) The fact that public confidence in the Bank would be reduced if the Bank did not deal exclusively with

eligibility of premium and private clients using advisory services

test data, remote and potential danger to avoid

does not require the processing of personal data.

(69) In view of the above, the Bank did not demonstrate in the balancing test that it was prudent

to meet the requirements of its group of companies

why compliance requires the use of a non-advisory service only

manage the personal information of your premium and private customers in the aptitude test.

Other comments on the balancing test

(70) In the 'Proportionality test' section of the balancing test, the Bank found that

data management is carried out in a way that is transparent to the data subjects, as the data subject is subject to the

provisions of the Bszt.

shall be required to make available to the Bank in accordance with the relevant provisions of

their personal data, of which the Bank duly informs them, so they can count on them

for data management. In addition, according to the Bank, the target market for the investigation is

those concerned should in any case provide the personal information provided in the aptitude test

their data to the Bank, therefore they do not use a separate questionnaire, but are provided in the test

use data for this purpose.

(71) The Bank has not specified here that Bszt. which provisions of its customers

handles your personal data on a mandatory basis and how you inform them. The

The Authority shall ensure the transparency and adequacy of the information provided on data management

Decision III.2. examined in point. In itself is that in some cases the Bank

The legal basis for the processing of personal data is the fulfillment of its legal obligation, it does not make it foreseeable a

Bank's data processing on other legal grounds.

(72) The Bank did not take part in the interest test or in the statements made during the procedure

explained exactly why you need the target market test to do so

for the processing of personal data, the processing of which is otherwise regulated by Bszt. it is not expressly prescribed

for. In the absence of this derivation, neither the need for data management nor its need

proportionality is not supported.

(73) The balancing test III.3. use only non-advisory services

personal data provided by the customer in the suitability test of premium and private customers

management involves a medium risk for customers. In this connection, the Bank did not decide
the scale on which it identified data management as medium risk
examples of what data processing is considered low or high risk, these are
and in its absence, the risk classification of data management is not justified, so the risk
the adequacy of the classification cannot be judged.

(74) The balancing test III.11. supports the proportionality of data processing,
that the exercise of the rights of the data subject is ensured, IV.1. and at all times
they may exercise their right to protest.

(75) The Bank provides information on the rights of the data subject in Section 8 of the Data Protection Prospectus. THE
with regard to the right to protest, explains that the right to protest can be exercised at any time, “if
the legal basis is the legitimate interest (…), unless there are compelling legitimate reasons to process the data,
which take precedence over the rights of the data subject or to bring legal actions,
related to the enforcement and protection of

(76) As explained by the Authority in paragraph 96 of this Decision, the Bank is nowhere to be found
provided information to its non-advisory clients
that the personal data they provide in the aptitude test is in their legitimate interest
they may not be aware that they may object to the processing, for example
however, one of the aspects taken into account when examining the proportionality of data management is not
is met.

(77) In addition to the above, the Bank stated in its submissions during the procedure that:
it would be unrealistic to have a framework contract with premium and private customers only
would complete the aptitude test, as the provision of investment advice to them is a
is part of day-to-day administration. The Bank's argument involves a balance of interests
test did not appear, but the Authority considers it important to record that convenience considerations
they do not in themselves legitimize a data processing if the service provided
no personal data processed is required to use it.

(78) On the basis of the above, the Authority concludes that the Bank has a legitimate interest in data processing

the need to assert its interests in the balancing test and the

other statements made in the proceedings

may lawfully invoke Article 6 (1) (f) of the GDPR as a legal basis for data processing,

that is, in the aptitude test of its non-advisory clients

handles the personal data you provide without any legal basis.

III.1.3. Performance of contract

(79) In its statement dated 31 May 2019, the Bank referred to Article 6 (1) (c) and (f) of the GDPR.

processing of personal data included in MiFID questionnaires

also referred to Article 6 (1) (b) of the GDPR as the legal basis, according to which this information

are required

the

investment

service

framework contract

and or

Treasury

to perform the services covered by the framework contract.

(80) In this respect, the Authority notes that the Bank only referred to the above as a legal basis for the processing of personal

data in MiFID tests.

referred to in the balancing test or in the various prospectuses (Privacy Policy)

information; Investment Business Rules, Client Information) no.

18

(81) Only personal data may be processed with reference to a contractual legal basis which:

essential for the performance of the contract, i.e. data management and the contract

there must be a direct and objective link between the purpose for which it is to be performed. By customers a

within the framework of a framework contract for the use of investment services

in the absence of the investor protection rules contained in the Bszt.

the data from the compliance and suitability test would not be required because

for example, it is not necessary for the Bank to buy a security for the customer

know what your highest level of education is.

(82) The legal basis of the contract is not applicable in cases where the processing is in fact

it is not due to the performance of the contract but to the fulfillment of a legal obligation on the controller

need.

(83) Management of investment firms' compliance and suitability test data

their legal obligation as defined in the Bszt., the purpose of which is to protect investors,

that is, ensuring that the client's investment firm only has a product

offer for sale or sell a product that, among other things, satisfies the customer

preferences, load-bearing capacity and risk-taking.

(84) Due to the above, the personal data included in the compliance and suitability tests are not

may be managed on the basis of a contract between the Bank and the customer in order to fulfill it, but

Article 6 (1) (c) of the Bank's GDPR and Bszt. Section 44 (1) and Section 45 (1)

shall be treated in accordance with its legal obligation under

(85) Section III.1. Summarizing the findings made in point 1, the Authority concludes that the Bank did not

has a legal basis for clients using only non-advisory services a

processing of personal data provided in the aptitude test, in breach of the

Article 6 (1) of the GDPR.

III.2. Information on the handling of personal data recorded in MiFID tests

(86) The Bank provides information to stakeholders on the processing of personal data recorded in MiFID questionnaires in

various documents. The Authority shall provide

During the examination of information, the Data Protection and Data Management

Information leaflets (hereinafter: Privacy Statement) can be found on MiFID tests

information, the framework agreements applied by the Bank, 1 January 2018 and April 2019

22 of the Investment Business Rules (hereinafter: the Business Rules) and the Bank

prospectus for investment services provided by

Customer Information).

(87) During the period under review, the Bank had two valid Data Protection Notices, the first being in 2018.

it entered into force on 25 May 2018, the second replacing the previous one on 10 July 2018. The latter

It was valid until June 17, 2019. Both current and past Privacy Policy

prospectuses are available on the Bank's website.

(88) In several documents, the Bank has fragmented content that is not identical but partly overlapping

provides information on the handling of personal data included in MiFID questionnaires, so a

the information in different documents are all relevant.

(89) The two Data Protection Data Sheets at different times contain the same information on the handling of personal data

recorded in MiFID tests and should therefore be provided by the Authority in a uniform manner.

treats it as a document.

19

(90) The Bank provides information in the Data Protection Prospectus on, inter alia, data management

the legal basis of the data, the purpose of the data processing, the scope of the processed data. The Investment Business

Rules

II.6. The information in section 1 is partly data protection and is defined therein

the purpose of the data management and the range of data recorded in the MiFID tests are partly specific and partly

generally defined.

Content requirements

Information on the legal basis for data processing

(91) Pursuant to Article 13 (1) (c) of the GDPR, where personal data are collected from a data subject

the controller must inform data subjects of the legal basis for the processing. The GDPR 13.

and Article 6 (1) (d) if the processing is covered by Article 6 (1) of the GDPR

(f), the legitimate interest of the controller or of a third party shall also be

stakeholders.

(92) The Bank provides information on data management in Section 2 of the Data Protection Information

legal basis. The Bank informs the interested parties that “Provided by the Bank

data processing related to services is usually of a mixed legal basis, ie both

include contractual, statutory and discretionary interests and

data management authorizations based on the consent of the Customer or other stakeholders. " This

After that, the Bank summarizes the legal bases applied by it in the Data Protection Prospectus

However, these definitions are of a general nature and do not show that

specifically in relation to the provision of investment services, included in the MiFID questionnaires

the legal basis on which the Bank handles personal data.

(93) Article II.6 of the Business Rules. of the Customer's product knowledge and risk bearer

under the heading “The Bank is included in the Bszt

prior to the provision of investment services in accordance with its obligation

requests a statement on the substance of the transaction included in the contract, the financial involved in the transaction

knowledge of the characteristics of the device, and in particular its risks, and

(hereinafter referred to as the compliance test) (…). " In compliance tests, the

The legal basis for the processing of personal data provided by data subjects is therefore the Business Rules

according to the legal obligation of the Bank, however, the data recorded in the aptitude tests

does not cover the legal basis for its management.

(94) According to point 4 of the Customer Prospectus, “Bszt. the Bank is obliged to invest

prior to the provision of advisory and portfolio management services

The Client or the person acting on behalf of the Client is related to financial instruments

knowledge, risk-bearing capacity, income position and investment objectives. On this

information to the Customer in the so-called When completing the Suitability and Compliance Test, you can bring a

Bank note (…). Investment advice and portfolio management services

for the use of other investment services and ancillary services other than

the Customer must complete the Compliance Test. ” Thus, in the Customer Prospectus a

Bank informs stakeholders in the case of investment advice and portfolio management

legal obligation to handle the personal admission to the aptitude and compliance test

data. However, it is not clear from the Prospectus that the investment

services other than consultancy and portfolio management

in the case of legal relations for the performance of the contract between the data subject and the Bank, the Bank shall be legal

necessary to fulfill the obligation or to enforce the legitimate interest of the Bank a

Completion of compliance test.

(95) The Bank is the first in the MiFID - Investor Questionnaire - Individuals

on both sides, both before the aptitude test and the compliance test, immediately before

20

after the identification data section, it informs the interested parties that “included in the Bszt

based on its obligation to provide prior information, has completed the following questionnaire for its customers

Who." From this wording it can only be concluded that the Bszt. according to

obligation not only to complete the questionnaires but also to provide the personal information provided

data processing.

(96) In contrast, the Bank's statements to the Authority and the balance of interests

the processing of personal data included in the compliance test as described in the

the legal basis of the Bank's legal obligation for all customer categories and service types

while the legal basis for the processing of personal data included in the aptitude test is only

it is its legal obligation if it provides advisory services or, failing that, the Bank

legitimate interest.

(97) It is by no means clear from the Data Protection Prospectus that specifically in MiFID tests

what is the legal basis for the processing of personal data provided, even though its name is

interested parties should primarily read this document if they wish to inquire about the Bank

data management by the The Business Rules already include that in the compliance test

The Bank manages the data provided on the basis of its legal obligation and records the same

for suitability and compliance testing, the Prospectus is advisory

services (investment advice and portfolio management). One

however, neither document contains information that the premium or private

for customers in the customer category using only non-advisory services

handles the personal data provided in the aptitude test on the basis of the legitimate interest of the Bank, and

it is not stated what this legitimate interest is.

(98) Consequently, the Bank infringed Article 13 (1) (c) and (d) of the GDPR by failing to

provided information that data processing was in its legitimate interest in certain cases

necessary to enforce and did not specify what this legitimate interest is.

Formal requirements

(99) Article 12 of the GDPR sets out the formal requirements to be met

be controllers when they allow the data subject to exercise their rights, ensure that

including prior information to stakeholders. This is based on the personal data of the data controllers

all information on data management is concise, transparent, comprehensible and easy to use

in an accessible form, in a clear and comprehensible manner.

(100) The Bank provides information on several levels, in several documents, as provided in the MiFID tests

on the processing of personal data. The Privacy Notice is for general information only

it does not state on what legal basis and for what purpose the Bank handles the personal data provided in the MiFID tests.

(101) There are four different legal bases for the processing of personal data recorded in MiFID tests

information is scattered throughout the document, with different contents. That way

the information provided is too fragmented and the Bank entrusts the task of

that there is a jigsaw puzzle on the legal basis for data processing in the various documents

pieces are assembled and it is understood from the resulting - incomplete - picture that the Bank a

the legal basis on which they handle their personal data provided in the compliance and suitability test.

(102) The Bank did the same when informing about the purpose of data processing. The Privacy Policy

According to point 3 of the prospectus, “The exact purpose for which the Bank, if any, or

manages the data of the data subject for the purposes of governing the contractual relationship between the Bank and the

Customer

Terms and Conditions - the applicable Business Rules for the product or service

21

and the specific contracts entered into with the Customer, and

statements and prospectuses relating thereto. "

(103) The Data Protection Bulletin does not contain specific data management purposes, an indicative list

such as “performance of a service contract between the Bank and the customer,

performance of a contracted service '; “With the Bank or with the Bank

enforcement and protection of the legitimate interests of related third parties'; "other,

compliance with statutory data management obligations', etc. The

Business rules II.6. and Section 4 of the Prospectus already states that

the purpose of the processing of personal data recorded in aptitude and compliance tests.

(104) The Code of Conduct is a fifty-page document that does not contain data protection

relevant section or point, but also relevant to the data management under consideration

information is placed in the section entitled General Terms and Conditions of the Services in Section II.6.

Examination of the Customer's product knowledge and risk-bearing capacity.

(105) The Prospectus provides a brief summary of the investment services provided by the Bank

services, but it does not explicitly include a data protection clause or chapter,

the provisions relevant to the data processing examined in this document are

They can be found under the title Assessing the client's risk-bearing ability and market knowledge.

(106) The requirement of transparency implies that Article 13 of the GDPR is expected to apply

information should be clearly separated from all non-data protection

information, e.g. contractual provisions.

(107) The Bank does not provide transparent information on the handling of personal data recorded in MiFID questionnaires

information as the Privacy Notice, which is named primarily

it should contain information related to the processing of personal data, too

general, it does not indicate the circumstances of the specific data management. More precise

information is contained in the Business Rules and the Customer Prospectus, although the

The purpose of the customer prospectus is for the Bank to provide general, concise, easy-to-understand information

certain clients related to the investment services it provides to its clients

rights and obligations of the Bank. The Business Rules are general

contains terms and conditions of service from which the

data protection information.

(108) In view of the above, the Bank's handling of personal data included in the MiFID questionnaires

infringed Article 12 (1) of the GDPR in so far as it

the information provided does not meet the requirement of transparency.

III. 6. Legal Consequences

(109) The Authority condemns the Bank under Article 58 (2) (b) GDPR for:

infringed Article 6 (1), Article 12 (1) and Article 13 (1) of the GDPR.

paragraph.

(110) Pursuant to Article 58 (2) (d) of the GDPR, the Authority instructs the Bank to cancel

the personal data provided in the aptitude test for premium and private customers who

they do not use the Bank's investment advisory or portfolio management services;

and adapt its disclosure practices to comply with Article 13 of the GDPR.

requirements of Article

(111) The Authority has examined whether it is justified to impose a data protection fine on the Bank.

In this context, the Authority will amend Article 83 (2) of the GDPR and Infotv. 75 / A. §

considered all the circumstances of the case. In view of the circumstances of the case and the fact that the Debtor has not violated the provisions of the GDPR for the first time (NAIH / 2019/2074), therefore, the Authority found that in the case of the infringements detected in the present proceedings, a warning is neither a disproportionate nor a dissuasive sanction, including the imposition of a fine required.

(112) NAIH / 2019/2074/22. In its decision no., the Authority found that the Bank infringed Article 6 (1) of the GDPR, as the personal data of the requesting customer - a on the prevention and deterrence of money laundering and terrorist financing 2017 LIII. Section 7 (2) of the Act and Act C of 2000 on Accounting. affected by the preservation obligation specified in Section 169 (2) of the Act with the exception of personal data - as of 25 May 2018, unlawful, appropriate without a legal basis.

(113) In imposing the fine, the Authority took into account the following factors:

(114) In particular, the Authority noted that the infringements committed by the Bank were In accordance with Article 83 (5) (a) and (b), it falls within the higher category of fines constitute an infringement.

(115) In setting the fine, the Authority took into account as an aggravating circumstance that:

•

•

•

•

the infringement is of a continuous nature and persisted during the period under investigation [GDPR Article 83 (2) (a)];

the infringement affects a large number of persons concerned [Article 83 (2) (a) GDPR]:

o no information on the processing of personal data included in MiFID questionnaires Infringement committed with due notice by the Bank of all investment

affects the number of customers using the service on 31 May 2018

[…], On December 28, 2018, was […] principal;

o the number of persons involved in unlawful data processing is not exactly

can be determined because the Bank does not record what service it received

resort to your customer, but what kind of transaction, but from 1 January 2018

there were a total of […] clients eligible for advisory services, but

no advisory transaction. As a result, the number of people affected by the infringement

presumably […] people.

inadequate handling of personal data recorded in MiFID questionnaires

information has indirectly impeded the exercise of the right of customers to

whose personal data included in the aptitude test is in the legitimate interest of the Bank

as the Bank did not provide them with personal information anywhere

the legal basis for the processing of their data [Article 83 (2) (k) GDPR];

information on the handling of personal data recorded in MiFID questionnaires

its opacity is a serious infringement because it is such a specialized professional

The Bank should provide information on data management related to these issues to the

data subjects to which the average data subject cannot have access from other sources, thereby

on the management of data relating to the provision of investment services

information is of paramount importance [Article 83 (2) (k) GDPR].

(116) The Authority took into account as a mitigating circumstance that the Bank had a legitimate interest

as one of the purposes of its processing and as a legitimate interest in the processing

enhanced investor protection [Article 83 (2) GDPR

the dot].

23

(117) The Authority also took into account the data breaches identified

are considered to be negligent in the absence of circumstances indicating intent [GDPR 83.

Article 2 (2) (b)] and do not affect specific categories of personal data

[Article 83 (2) (g) GDPR].

(118) In both case number […] and in the present case, the Authority found that Article 6 (1) of the GDPR

However, on the basis of different circumstances in the two cases, the Bank

infringement of the same provision of the GDPR in relation to its various activities

to establish. As a result, the Authority has examined the Bank's previous conduct

infringement, but is not relevant in the context of the present proceedings

the Authority did not consider it to be an attenuating or aggravating circumstance

in determining the amount of the fine. [Article 83 (2) (e) GDPR].

(119) The Authority did not consider the imposition of a fine to be relevant under Article 83 (2) (c), (d),

circumstances set out in points (f), (h), (i) and (j), as they do not apply in the specific case.

can be interpreted.

(120) According to the Debtor's consolidated financial statements for 2018, its pre-tax profit is 27,598

million, and its profit after tax was HUF 24,056 million, ie the amount of the fine

does not reach one thousandth of the Debtor's pre-tax profit. The privacy imposed

the amount of the fine does not exceed the maximum fine that may be imposed.

(121) In view of the above, the imposition of a fine is necessary for the Bank specifically or

other similar breaches in general for similar data controllers

to prevent.

(122) The amount of the fine was determined by the Authority in accordance with its statutory discretion

me.

(123) The Authority Pursuant to Section 61 (2) (a), the Bank shall order the decision

disclosure of his identification data since the decision

affects a wide range of people.

(124) On the basis of the above, the Authority has decided in accordance with the operative part.

ARC. Other issues:

(125) The Authority's powers are governed by Infotv. Section 38 (2) and (2a), its jurisdiction is

covers the whole country.

(126) The decision is based on Article 80.-81. § and Infotv. It is based on Section 61 (1). The decision is

Ákr. Pursuant to Section 82 (1), it becomes final upon its communication.

(127) Art. Pursuant to Section 112 and Section 116 (1) and Section 114 (1) a

There is an administrative remedy against the decision.

(128) The rules of administrative litigation are laid down in Act I of 2017 on the Procedure of Administrative Litigation (a

hereinafter: Kp.). A Kp. Pursuant to Section 12 (2) (a), the Authority

The administrative lawsuit against the decision of the Criminal Court falls within the jurisdiction of the court. § 13

(11), the Metropolitan Court has exclusive jurisdiction. The civilian

CXXX of 2016 on the organization of litigation. Act (hereinafter: Pp.) - the Kp. Section 26 (1)

applicable within the jurisdiction of the General Court pursuant to § 72

legal representation is mandatory in litigation. Kp. According to Section 39 (6) - unless otherwise provided by law

the bringing of the action for the administrative act to take effect

has no suspensive effect.

(129) A Kp. Section 29 (1) and with this regard Pp. Applicable pursuant to Section 604, the

of 2015 on the general rules of electronic administration and trust services

CCXXII. Pursuant to Section 9 (1) (b) of the Act (hereinafter: the E-Administration Act)

the client's legal representative is obliged to communicate electronically.

(130) The time and place of the submission of the application are set out in Kp. Section 39 (1). THE

Information on the possibility of requesting a hearing is provided in the CM. Section 77 (1) - (2)

based on paragraph The rate of the fee for an administrative lawsuit is set out in the 1990 Fees Act

XCIII. Act (hereinafter: Itv.) 45 / A. § (1). The fee is preliminary

from the payment of the Itv. Section 59 (1) and Section 62 (1) (h) exempt

initiating proceedings.

(131) If the Debtor does not duly prove the fulfillment of the required obligation, a

The Authority considers that it has not complied with the obligation within the time limit. The Ákr. Section 132

if the debtor has not complied with the obligation contained in the final decision of the authority,

the executable. The decision of the Authority With the communication pursuant to Section 82 (1)

it becomes final. The Ákr. Section 133 enforcement - if you are a law

Government decree does not provide otherwise - it is ordered by the decision-making authority. The Ákr. 134.

§ pursuant to the implementation - if by law, government decree or municipal authority

In this case, the decree of the local government does not provide otherwise - the state tax authority

implements. Infotv. Pursuant to Section 60 (7) of the Authority,

to perform a specific act, to behave, to tolerate or

the Authority shall enforce the decision in respect of the standstill obligation

implements.

Budapest, November 15, 2019

Dr. Attila Péterfalvi

President

c. professor