Case number: NAIH / 2019/51/11.

(NAIH / 2018/4986 / H.)

Subject: Decision granting the application

Before the National Authority for Data Protection and Freedom of Information (hereinafter referred to as the Authority) […]

hereinafter: Applicant to the […] hereinafter referred to as the Debtor, his personal data is illegal

to establish the fact of the processing of personal data, to order the erasure of your personal data or personal data

initiated by the data protection authority to prohibit the unlawful processing of his data

take the following decisions in the procedure:

I. The Authority

IN ITS DECISION

1) the Applicant

grant your request

and finds that the Debtor is stored by the Applicant in violation of the principle of limited storage

private correspondence and, in breach of the principle of fair data management, adequate information

without the appropriate legal basis, contrary to the principle of purposeful data processing

search documents in your archived email accounts.

2) The Authority prohibits the Debtor from storing the Applicant's private correspondence

archives and instructs the Debtor to

within 30 days with the involvement and information of the Applicant, review that the Applicant is archived

Storing and Searching for Documents in the Offended, Defendant's E-Mail Accounts

personal data and correspondence not related to work (private)

became aware of or stored them and deleted them by opening an appeal against this decision

until the expiry of the statutory time limit for bringing an action or, in the case of an administrative action, the court is final

Until the decision of the

they may not be deleted or destroyed, however, during storage and in administrative litigation

they may not be used otherwise than by the court. In doing so, the Debtor

shall provide a copy of the data for private use only for the Applicant's own purposes

and shall be obliged to inform the Applicant about the data processing in respect of the undeleted data

properly informed.

3) The Authority shall establish of its own motion that the Debtor is in the archived e-mail accounts of the

Accountability is a fundamental principle in the handling of data related to document retrieval

has not taken appropriate technical and organizational measures in breach of

in order to use the e-mail accounts it provides to employees,

ensure the protection of personal data in connection with the archiving and did not take care of it

adequate information to stakeholders, in breach of the principle of transparency.

4) The Authority will instruct the Debtor ex officio to ensure that the decision becomes final

within 30 days of the entry into force of this Regulation

ensure that workers take technical and organizational measures in accordance with

use, archive, or access archived content

protection of personal data during document searches, create the necessary data

internal rules and ensure that those concerned are properly informed. In this context

ensure that you can store, archive, and search your archived data for email accounts;

internal regulations and by drawing up appropriate information on them,

archive employees 'email accounts and search for documents in them.

2

5) The Authority shall appoint the Debtor ex officio

HUF 500,000, ie five hundred thousand forints

data protection fine

obliges to pay.

***

The Authority shall impose a data protection fine within 15 days of the decision becoming final

centralized revenue collection target settlement forint account (10032000-01040425-00000000

Centralized direct debit IBAN: HU83 1003 2000 0104 0425 0000 0000)

to pay. When transferring the amount, NAIH / 2019/51. JUDGE. number should be referred to.

If the Debtor fails to meet its obligation to pay the fine within the time limit, the above

is required to pay a late payment surcharge on the account number. The amount of the late payment allowance is the statutory

interest,

which corresponds to the central bank base rate in force on the first day of the calendar half-year affected by the delay

me.

The Debtor is obliged to fulfill the obligations provided for in items I. 2) and I. 4) of this decision above

within 30 days of the date of notification of the decision - the supporting evidence

to the Authority.

In the event of non-compliance with the fine and the late payment allowance or the prescribed obligations, the Authority shall:

initiate the implementation of the decision.

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.

For those who do not benefit from full personal exemption, the judicial review process

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

Court

legal representation is mandatory.

II. The Authority shall order the payment of HUF 10,000, ie ten thousand forints, to the Applicant.

payment by bank transfer to a bank account of your choice due to the deadline being exceeded

or by postal order.

***

The present II. There is no place for an independent remedy against the order under point 1, it is only the case

may be challenged in an appeal against a decision on the merits.

EXPLANATORY STATEMENT

I. Procedure, clarification of the facts

I. 1. On 27 July 2018, the Applicant submitted an application to the Authority stating that

as director of […], he headed the institution until […] days. The employer's rights are the State

He was exercised by the director general of the Health Care Center. Following the termination of this legal relationship,

On July 2, 2018, through a current employee of the hospital, he learned that -

without your permission - hospital email sent before April 1, 2017

ordered the reinstatement of […] accounts which he had actually canceled and inactivated by [his] successor,

[…] Current leadership. On July 3, 2018, it was over the phone with the current medical director

during the conversation, the medical director admitted to the Applicant that he had given instructions to restore the email

accounts. During the restoration of these correspondence, the Applicant's former e-mail accounts

activated because they were looking for a document. The Applicant objected that in doing so a

have access to any of your documents in their accounts, any personal information

in view of the fact that he also carried out his private correspondence on them, he was also allowed to do so.

Thus, the accounts contained, for example, private correspondence, bank details, and payment information

data on friendships, information on the financial management of the Applicant

correspondence, bank account number, pin codes, health information, and

information on persons seeking medical care.

Act CXII of 2011 on the right to information self-determination and freedom of information. Act (a

hereinafter: Infotv.) at the request of the data subject

official proceedings have been initiated.

As the application did not contain any allegations concerning the alleged infringement

facts and evidence thereof and the decision to remedy the alleged infringement

application, the Authority called on the Applicant to

and requested a finding of unlawful processing of his personal data, his personal data

order the blocking, deletion or destruction of your personal data

prohibition of unlawful treatment.

The Authority also requested the Applicant to make a statement in order to clarify the facts,

who stated in his reply that […] as his former director of retention of e-mails

In order to do so, MailStore ordered the introduction of an e-mail archiving system, as it has occurred several times,

that the emails were mixed. Into this system of board correspondence

archived, including correspondence from the […] and […] accounts used by the Applicant, with two managers

there were those who were educated on its use. No special regulations on the operation of the system

due to the narrow circle of stakeholders, so only oral information was provided on its characteristics. THE

According to his statement, the applicant had the opportunity to have a legal relationship by agreement

use your […] email account for an additional month after

account. Your […] email account will expire on March 31, 2017

inactivated. The Applicant stated that he had so much information that he had email accounts

they are canceled, but have not been informed that their legal relationship has been terminated

after what happens to the contents of the accounts and about it - although he ordered the archiving system

nor did he have any information that the deletion did not mean that it would be

email accounts are deleted irrecoverably, but are deactivated.

I. 2. The Authority has notified the Debtor of the initiation of the official data protection procedure and

In order to clarify the facts, he was invited five times to make a statement or provide information.

According to the Debtor's statement, the e-mail addresses provided by the Applicant are institutional e-mail addresses,

or accounts in which the fact that the employer has also authorized their use for private purposes does not

therefore, a breach of the right to the protection of personal data is completely ruled out. THE

According to the Debtor's statement, they were given the opportunity to see the Applicant's legal relationship

delete your private mail, personal information, or at least one

He knew the date of his termination a month earlier, so he had the opportunity to

maintain your mailboxes. Furthermore, at the request of your mailboxes even after the termination of your legal relationship

could use it. The Debtor did not comment on the deadline, however, according to the Applicant
he had the opportunity to do so for one month after the termination of the legal relationship.

4

According to the Debtor's statement, of the e-mail addresses provided by the Applicant, […] is still
used, only its name has changed, updated and referring to the successor institution
[…], given that a succession took place on 31 March 2017
as a result, his predecessor […] ceased to exist and his successor became […].
According to the Debtor's further statement, the mailbox was not restored, but in the archive
they were looking for a legal document prepared by a contractual partner during which a document
was not saved. No report or record was made about the search.
According to the Debtor's statement during the term of the employment relationship with the Applicant
employees were not specifically informed about the use of email accounts, however
IT security policy contained the relevant rules. These rules are as follows
mean rules of conduct such as that letters cannot represent the force in force
conduct contrary to Hungarian law, letters must not offend the honor of others, human rights
rights, race, ethnicity, religious, political worldview. The content of the letters must not be infringed
copyright and related rights, the letters must not damage the reputation or reputation of the institution,
they may not intentionally disseminate false information about it or correspondence may not
may jeopardize the operation of the network infrastructure. Unsolicited mail and advertisements are also prohibited
sending or forwarding bombs or mail chains is prohibited. Leaves are prohibited
change your header, send fake emails. It is forbidden to send mail to any commercial
to be placed on a list from which the institution's mail system is being spammed.
The Debtor also stated that at the time of termination of employment, the employee
mailboxes are immediately deactivated unless the employee requests that the use of
be possible even after the termination of his employment and with the permission of the Director-General.
According to the Debtor's statement, deactivation of the electronic mailbox means that the account is a

no longer live, its contents are archived. The total processed, unchanged account content

considered an archive, this is where the document search took place. It is for the mailbox itself

however, deactivation does not affect mail that has already been processed and archived.

According to the Debtor 's statement, in order to back up the directories' mailboxes a

They use the MailStore email archiving system ordered by the applicant as a former director.

This system is set to save mail in […] and […] email accounts. The

archiving is done within a closed process as a unified database backup in such a way that

users do not have direct access to the archive. A MailStore

e-mails archived in the system remain available after the mailbox is deactivated, the archived

mails do not have a defined archiving time. Only with separate access from archived content

can remove mail. The purpose of introducing the MailStore system is

was to increase data security solely for the purpose of archiving board correspondence. The

given the small number of mailboxes actually involved in archiving - the Applicant has two e-mails

In addition to his mailbox, two other accounts were saved - all concerned were notified orally by

from the head of the IT department, and everyone involved was also aware that the contents of the accounts

will be retained indefinitely. Accurate use of the MailStore system for everyone

was taught by the administrator to show each affected computer how to do it

search the archive and retrieve accidentally deleted or shuffled mail from there. THE

In addition, according to the obligor's statement, the mailbox is in connection with the Applicant's employment

was a created work tool. The work tool is required for the work of the Applicant

the employer is responsible for ensuring compliance with Act I of 2012 on the Labor Code (a

hereinafter: Mt.) pursuant to Section 51 (1). Accordingly, the archiving of mailboxes

legal basis for the employment contract concluded with the Applicant and the work provided on the basis thereof

necessary condition.

5

According to the Debtor 's statement, the search in the archives of the institution' s organizational and

by the Deputy Director-General in accordance with its Rules of Procedure, orally, by letter dated 18 July 2018
took place on the day and took thirty minutes. According to the statement, the search is targeted, from
and according to the subject of the letter, of which the Applicant was not informed, as an employer
took place. Searching the archives of the two mailboxes is the institution's directorate-general
on the computer of his secretariat, using the web interface of the MailStore system. When searching
the Director-General of the institution shall be the Director of Medicine and another member of staff of the institution
an employee from the IT department was also present. However, the email you were looking for could not be found
in the archive, so no document was saved.

I. 3. Based on the statements, it can be stated that the introduction of the MailStore archiving system a
Appointed by applicant as former director. The Debtor has archived it in this system by the Applicant
the contents of your two private email accounts and then in this archive
document search is concluded with the Applicant, taking into account the provisions of § 11 of the Labor Code
employment contract as the legal basis relied on by the Debtor, the Applicant is preliminary
in the absence of information or presence, his legal relationship took place on 31 March 2017
in the year following its termination, on 18 July 2018. About using employee email accounts a
In accordance with the IT security policy referred to by the obligor, in addition to being permitted
have been used for private purposes and have defined certain principles for correspondence,
rules of conduct, handling of personal data of employees, and e-mail accounts
does not provide any information regarding the control and related data management
contain. The Applicant did not receive any information about the document search from the Debtor, only the
He became aware of this by notifying one of his obligated employees. Ordered by the Applicant
the archiving system, but the information on the order is available to the Authority
the exact characteristics of the system cannot be clearly established on the basis of this document or that
whether or not electronic mail can actually be deleted from it.

II. Documents examined by the Authority during the procedure:

-

[…] IT Security Policy (November 1, 2014)

-

[…] IT Security Policy (15/09/2017)

-

documents for ordering the MailStore archiving system

-

emails archived in the MailStore system from the email accounts used by the applicant

III. Applicable legal provisions

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

Article 2 (1) of Regulation (EU) No 2016/679 (hereinafter referred to as the General Data Protection Regulation)

the General Data Protection Regulation applies to personal data in part or

fully automated processing of personal data

which are part of a registration system,

or which are intended to be part of a registration system.

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

shall apply with the additions provided for in

Infotv. Pursuant to Section 60 (1), the enforcement of the right to the protection of personal data

the Authority shall, at the request of the data subject, initiate a data protection authority procedure.

Infotv. Pursuant to Section 60 (2), an application for the initiation of official data protection proceedings

Article 77 (1) and Article 22 (b) of the General Data Protection Regulation

may be submitted in a specific case.

Unless otherwise provided in the General Data Protection Regulation, data protection was initiated upon request

CL of the General Administrative Procedure Act 2016. Act (a

hereinafter: Ákr.) shall apply with the exceptions specified in the Information Act.

Pursuant to Article 99 (2) of the General Data Protection Regulation, the general data protection

It shall apply from 25 May 2018.

According to Article 4 (1) of the General Data Protection Regulation, “personal data” shall mean identified or

any information relating to an identifiable natural person ("data subject"); identifiable by a

a natural person who, directly or indirectly, in particular by an identifier, e.g.

name, number, location data, online identifier or physical, physiological,

genetic, intellectual, economic, cultural or social identity

identifiable by that factor. "

According to Article 4 (7) of the General Data Protection Regulation: "" controller "means the natural or legal person

legal person, public authority, agency or any other body that provides personal data

determine the purposes and means of its management, alone or in association with others; if the data management

purposes and means are determined by Union or Member State law, the controller or the controller

Union or Member State law may lay down specific criteria for the designation of

Under Article 5 (1) (e) of the General Data Protection Regulation: 'Personal data shall:

(a) be processed lawfully and fairly and in a manner which is transparent to the data subject

("legality, fairness and transparency");

(b) collected for specified, explicit and legitimate purposes and not processed

in a way incompatible with those objectives; not in accordance with Article 89 (1)

considered incompatible with the original purpose for the purpose of archiving in the public interest, scientific

and further processing for historical research or statistical purposes ("purpose limitation");

(e) stored in a form which permits identification of data subjects for personal purposes only

allows the time necessary to achieve the purposes of data processing; personal information than this

longer storage can only take place if personal data

in accordance with Article 89 (1) for archiving in the public interest, scientific and

will be carried out for historical research or statistical purposes, those covered by this Regulation

appropriate technical and organizational arrangements to protect their rights and freedoms

subject to the implementation of measures ("limited storage capacity"). "

According to Article 5 (2) of the General Data Protection Regulation: “The controller shall be responsible for

shall be able to demonstrate such compliance

("Accountability"). "

Under Article 6 (1) of the General Data Protection Regulation: “Processing of personal data

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

(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 one of the parties is a party; or

to take steps at the request of the data subject before concluding the contract

required;

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

(d) processing is in the vital interests of the data subject or of another natural person

necessary for its protection;

(e) the exercise of a public interest or the exercise of official authority vested in the controller

necessary for the performance of its task;

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

necessary, unless the interests of the data subject take precedence over those interests

or fundamental rights and freedoms which call for the protection of personal data,

especially if the child concerned. "

Under Article 13 (1) to (2) of the General Data Protection Regulation: '(1) If the data subject

personal data are collected from the data subject, the controller shall process the personal data

provide the following information to the data subject at the time of acquisition

each of them:

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

(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 a third party

legitimate interests of a party;

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

(f) where applicable, the fact that the controller is a third country or international organization

personal data and to the Commission’s compliance decision

existence or absence thereof, or in Article 46, Article 47 or the second subparagraph of Article 49 (1)

in the case of the transfer referred to in the first subparagraph, an indication of the appropriate and suitable guarantees,

and the means by which copies may be obtained or made available

reference.

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 data management

provide the data subject with the following additional information:

(a) the period for which the personal data will be stored or, if that is not possible, that period

aspects of its definition;

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

access, rectification, erasure or restriction of their processing and may object to such

against the processing of personal data and the right of the data subject to data portability;

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

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

does not affect the lawfulness of the processing carried out on the basis of the consent prior to the withdrawal;

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

(e) that the provision of personal data is required by law or by a contractual obligation

based on or a precondition for concluding a contract and whether the person concerned is obliged to be personal

data and the possible consequences of providing the data

failure;

(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 processing and on the data subject

its expected consequences. "

According to Article 21 (1) of the General Data Protection Regulation: “The data subject shall have the right to:

at any time on grounds relating to his or her situation, object to the processing of his or her personal data in accordance with

Article 6 (1).

based on those provisions, including those provisions

based profiling. In this case, the data controller may not process the personal data

unless the controller demonstrates that the processing is justified by compelling legitimate reasons.

justified by the interests, rights and freedoms of the data subject

or to bring, assert or defend legal claims

are related. "

Under Article 26 of the General Data Protection Regulation: '(1) Where the purposes and means of data processing are twofold

or jointly determined by several controllers, they shall be considered as joint controllers. The common

data controllers shall define this Regulation in a transparent manner in an agreement between them

obligations, in particular the exercise of the rights of the data subject and the

and their responsibilities for providing the information referred to in Article 14

the division of their related responsibilities, unless and to the extent that

the division of responsibilities for data controllers under Union or Member State law applicable to them

Define. The agreement may provide for a contact person for the parties concerned.

2. The agreement referred to in paragraph 1 shall reflect the common controllers

their role vis-à-vis stakeholders and their relationship with them. The essence of the agreement is concerned

shall be made available.

3. The data subject shall be independent of the terms of the agreement referred to in paragraph 1

data controller and against each controller

rights under this Regulation. "

According to Article 32 (1) (c) of the General Data Protection Regulation: “The controller and the

the state of the art in science and technology and the cost of implementation; and

the nature, scope, circumstances and purposes of the processing and the rights of natural persons; and

taking into account the varying probability and severity of the risk to

implement appropriate technical and organizational measures to address the risk

guarantees an adequate level of data security, including, where appropriate:

in the event of a physical or technical incident, the ability to access personal data

access and availability of data can be restored in a timely manner. "

According to Article 58 (2) of the General Data Protection Regulation: “The supervisory authority shall be corrective

acting under the authority of:

(a) warn the controller or processor that certain data processing operations are planned

its activities are likely to infringe the provisions of this Regulation;

(b) condemn the controller or the processor if he or she has breached his or her data processing activities

the provisions of this Regulation;

(c) instruct the controller or processor to comply with the data subject's obligations under this Regulation

request for the exercise of his rights;

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

in a specified manner and within a specified period, in accordance with the provisions of this Regulation;

(e) instruct the controller to inform the data subject of the data protection incident;

(f) temporarily or permanently restrict the processing, including the prohibition of the processing;

(g) order personal data in accordance with Articles 16, 17 and 18 respectively

rectification or erasure of data and restrictions on data processing, as well as Article 17 (2)

shall notify the addressees with whom it is addressed in accordance with paragraph 1 and Article 19

or with whom personal data have been communicated;

(h) withdraw a certificate or instruct a certification body in accordance with Articles 42 and 43

revoke a certificate issued by the. or instruct the certification body not to issue the

a certificate if the conditions for certification are not or are no longer met;

(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; and

(j) order the flow of data to a recipient in a third country or to an international organization

suspension. "

Under Article 83 (2), (5) and (7) of the General Data Protection Regulation:

9

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

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

whether it is necessary to impose an administrative fine or the amount of the administrative fine

In each case, due account shall be taken of the following:

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

the nature, scope or purpose of the infringement and the number of persons affected by and affected by the infringement

the extent of the damage suffered;

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

(c) the mitigation of damage caused to the data subject by the controller or the processor

any measures taken to

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

and the technical and organizational measures taken pursuant to Article 32;

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

(f) the supervisory authority to remedy the breach and the possible negative effects of the breach

the degree of cooperation to alleviate

(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 that:

whether the breach was reported by the controller or processor and, if so, what

in detail;

(i) if previously against the controller or processor concerned, on the same subject matter

- has ordered one of the measures referred to in Article 58 (2), the person in question

compliance with measures;

(j) whether the controller or processor has kept itself approved in accordance with Article 40

codes of conduct or approved certification mechanisms in accordance with Article 42;

and

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

financial gain or avoidance as a direct or indirect consequence of the infringement

loss.

[…]

5. Infringements of the following provisions in accordance with paragraph 2 shall not exceed 20 000 000

With an administrative fine of EUR 1 million or, in the case of undertakings, the previous financial year in full

up to 4% of its annual worldwide turnover,

the higher amount shall be charged:

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

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

(c) the transfer of personal data to a recipient in a third country or to an international organization

transmission in accordance with Articles 44 to 49. in accordance with Article

d) the IX. obligations under the law of the Member States adopted pursuant to this Chapter;

(e) the instructions of the supervisory authority pursuant to Article 58 (2) or the temporary processing of data

or a request to permanently restrict or suspend the flow of data

failure to provide access in breach of Article 58 (1).

[…]

7. Without prejudice to the corrective powers of the supervisory authorities under Article 58 (2),

each Member State may lay down rules on the

whether an administrative or other body performing a public function may be imposed

fine and, if so, the amount. "

Under Article 88 (1) and (2) of the General Data Protection Regulation:

1. Member States shall specify this in legislation or in collective agreements

rules may be laid down to ensure the protection of rights and freedoms

with regard to the processing of employees' personal data in connection with employment,

in particular recruitment for the purpose of fulfilling an employment contract, including in law

or collectively agreed obligations, work management,

planning and organization, equality and diversity in the workplace, the workplace

health and safety, the protection of the employer 's or consumer' s property, and

the individual or collective exercise and enjoyment of employment-related rights and benefits

for the purpose of termination of employment.

2. These rules shall include appropriate and specific measures which are appropriate

to protect the human dignity, legitimate interests and fundamental rights of the data subject, in particular

transparency of data management within a group of companies or a joint economic activity

intra-group transfers and on-the-job checks

systems.

[…] ”

Infotv. 75 / A. "The Authority shall, in accordance with Article 83 (2) to (6) of the General Data Protection Regulation,

shall exercise the powers set out in paragraph 1, taking into account the principle of proportionality, in particular:

by the law on the processing of personal data or by the European Union

in the event of a first breach of the requirements laid down in a mandatory act of the

in accordance with Article 58 of the General Data Protection Regulation

take action by alerting the controller or processor. "

Infotv. Pursuant to Section 61 (4) (b): “The amount of the fine is from one hundred thousand to twenty million forints

may apply if the payment of a fine imposed in a decision in an official data protection procedure

budgetary body, a fine imposed pursuant to Article 83 of the General Data Protection Regulation

in case of."

ARC. Decision

ARC. 1. General findings

Available to the employee according to the definitions in the General Data Protection Regulation

the data content of the workplace e-mail account provided is personal data, performed on the personal data

and any operation is considered data management. A separate issue is that personal data,

or the data processing is exclusively related to the work, its purposes or for private purposes

which occurs when assessing the identity of the data controller and the lawfulness of the data processing

may be relevant.

In the present case, on the basis of the statements and the attached documents, it can be concluded that a

The so-called “corporate e-mail accounts” provided by the Debtor and used by the Applicant were also used by the Applicant

for private purposes, their use for private purposes was also permitted.

for.

In the case where an employee uses an email account - regardless of whether

the employer otherwise prohibits or authorizes private use - stored in it

with regard to personal data, it itself carries out data management activities.

Where the processing is connected with the performance of the work, it shall be for the purpose of:

the employee acts essentially on behalf of the employer as data controller and his activity as

data processing activities can also be attributed to the employer. That this data management a

to the extent that it is lawful for persons other than the employee, regardless

and the liability for any illegality depends on whether

necessary and appropriate technical and organizational arrangements made by the employer as data controller

non-compliance with the measures by the employer or the absence of such measures as a result of

that, in relation to third parties, in accordance with the relevant civil law rules, the

employer is responsible.

With respect to the employee's own personal data, as long as data processing is the job

the legal basis for data processing in the case of an employment relationship

above all, the employment contract and the data processing must be judged accordingly. That's it

however, as in the present case, when performing a task in the public interest or a public authority

it is an exercising body, data controller, the legal basis of data management in the case of this data management is

the legal basis under Article 6 (1) (e) of the General Data Protection Regulation that a

the processing of personal data is lawful if the processing is in the public interest or to the data controller

in the exercise of a public authority conferred on it

required.

However, in the case of an employee with an email account provided by the employer

also carries out activities which are not related to the performance of work - for private purposes and in connection with which

the

handles the personal data of itself and, in most cases, other third parties, is no longer the case

the situation is clear. In this case, the purpose of the data processing is not determined by the employer

but also the employee, who may, where appropriate, become the data controller himself

in no way related to your work with regard to the personal data of individuals

data management. He decides whether to include personal information in his email account and until

In the possession and control of the account, you can decide to delete it or use it in the meantime.

However, the operation of the system for these personal data continues to be a

the duties and powers of the employer and the disposition of the e-mail account that stores personal information

nor does the employer lose his right to remain a data controller for private data.

The same applies, where appropriate, to the security of work-related e-mails

it is also the result of the employer 's decision and the quality of the employer' s data controller that a

the entire contents of your employee email account, including private emails, are consistent

archived and stored by the employer as a database.

The quality of the employer 's data controller cannot be questioned in this case either, because a

with the express permission and knowledge of private use

as a result of which they may be placed for a purpose which he has determined for himself

to an email account used for data management with other employee data management

personal data, which on the one hand are actually related to their own data processing

also through persons acting. On the other hand, due to the circumstances of data management

it is actually possible to manage the personal data in the e-mail account that it has

they do not really have any connection with the processing of data for a controlled purpose - which is a

can almost never be ruled out as a work tool for a work email account or mobile phone

and in the case of other computer equipment provided, although would be expected, the cases

the employer is expected to expect - in his own data management

all data processing carried out in the framework of the fulfillment of the necessary requirements for

its activities necessarily extend to this data (above all, it stores it) and its own

in the performance of its tasks necessary to ensure the lawfulness of its data processing

to this personal information.

It should also be noted that, as long as the employee is concerned, the processing of such data stored in the email account

solely for his or her private interest, i.e. for private purposes, may be

as data processing exclusively in the context of a personal or domestic activity is excluded

within the scope of the General Data Protection Regulation, this may not be the case for the employer. The

in such cases, therefore, a very specific joint data processing situation arises, in which case the

in any case, the employer qualifies as a data controller and the employee in a legal sense

at least - not necessarily.

In addition to the above, it is also important that due to the legal relationship between the employer and the employee
the employer has the primary responsibility for the lawfulness of the data processing, as for him
primarily available tools (internal regulatory and technical operational
measures) to ensure legality. So it is his responsibility to recognize this situation,
and appropriate employer measures to deal with it, including in the case of joint data management
agreement on the details of data management, the responsibilities related to data management
its regulation (essentially in accordance with Article 26 of the General Data Protection Regulation).
Finally, it is essential that the employee’s personal information is private
the employer is considered to be a data controller, it does not mean that such
The processing of personal data processed for this purpose by it is lawful in all cases, since if a
no lawful purpose of the processing of such data can be identified on the employer 's side, or
Article 6 (1), there will be no out-of-storage processing of such data
lawful, such personal data may not be used by the employer. The plea is unfounded
The general legal consequence of data processing is that the employer, as soon as
is informed of the processing of such data - terminates the processing of such data, ie deletes them
from your email account. However, in a situation such as the present, the erasure of the data as
data processing operation - especially if the employee would actually be a joint data controller
may be considered, where appropriate, solely in the interests of the employee, and
above all by complying with the requirement of fairness of data processing
can be legally achieved.
In this respect, the employer, as data controller, must first of all inform the
the employee of the intended data processing operation and give him the opportunity to
control the handling (deletion) of data, and - if the data in question are deleted, they are a
would no longer be available to the employee - not by the employer
save manageable data to your own device. By definition, the employer is legal

with regard to the data subject to its data processing - which is the responsibility of the employer as data controller

obligations, in particular data security requirements, and such data backup

the employer has the right and obligation to supervise that it is in fact only the

limited to data processed for private purposes. Establishing a procedure and mechanism and

implementation is therefore required where possible both parties control the data

The process of ‘sorting out’, and in doing so only the data that it cannot legally process

to determine this quality of data, the most necessary scope to control the process

be limited.1

In the light of the above, the personal data of that employee must be judged by the employer

who, in addition to using your e-mail account for work purposes, also

use the email account provided by your employer.

In such situations, the lawfulness of data processing is subject to data protection requirements

its adequacy in this respect shall be assessed in accordance with the above.

Even if the employer explicitly allows private use as a data controller, it will still only be

lawful processing on the part of the data subject, if appropriate, in accordance with Article 6 (1) of the General Data Protection

Regulation

has a legitimate basis. However, such a permit alone is not enough, it requires the employee

accurate information on the details of such data processing, in agreement with the employee, is effective

settlement in the form of an agreement - depending on whether the employee is only about the data or by a third party

whether it is also the processing of personal data.

1

13

ARC. 2. Email archives containing private mail

ARC. 2. 1. General remarks

The Applicant objected that in the year following his legal relationship terminated on 1 April 2017, 2018

in July, without your consent - hospital electronic generated before April 1, 2017

your mail has been restored to restore your deactivated email accounts to your current job

leadership because they were looking for a document. According to the Applicant's statements in the accounts of his and

the Debtor may have accessed the personal data and private correspondence of other persons.

The present case concerns two data processing operations. One of the Applicant's private letters

storing archives of e-mail accounts that contain, the other searching the archives. THE

In his request, the applicant essentially objected to the search in his archived e-mail accounts,

however, given that the two data processing operations are interlinked, the search,

would not have been possible without storing the email accounts, so the Authority

it also examined the legality of the retention of electronic mail.

When reviewing the contents of archived e-mail accounts sent by the Debtor to the Authority

the Authority has established that the e-mail accounts used by the Applicant, its correspondence, the

a number of private correspondence (such as family trees, among others, and

friendly correspondence), so by obliging the Applicant to archive the Applicant’s e-mail accounts

The Applicant has stored and continues to store personal data contained in these private letters,

or searched them.

ARC. 2. 2. Purpose and legal basis of data processing

The Obligor aims to increase data security for the purpose of archiving electronic mailboxes

which is generally recognized by the Authority as an appropriate, legitimate data processing purpose, as the

related to certain work required for office operation and work

You must keep documents and restore them in the event of a data security issue

to ensure the continuity of work processes.

The Authority considers that, where applicable, employees' e-mail accounts used for private purposes are acceptable

storage of its contents for the reason that it is necessary for the operation and work of the office

documents are required to ensure the continuity of work processes

but must have an appropriate legal basis for doing so, and

a distinction should be made between the contents of the letters according to their dependence on work

these are private emails.

For these purposes, both employment and private correspondence during the employment relationship

Article 6 (1) (e) of the General Data Protection Regulation

allows for backups, also with regard to information security rules, which

According to the legal basis, the processing of personal data may be lawful even if the processing is in the public interest

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

necessary for its implementation.

After the termination of the employment relationship, they can also be archived and managed for this purpose and on the basis

of a legal basis

electronic mail. However, the specifically private correspondence is also given that

their treatment on the part of the employer may not be necessary in any way, as a general rule

cannot be archived. The Authority would then accept such correspondence as mere

storage, to the exclusion of all other data processing operations, for backup purposes if the

as a single database for saving business and private mail

sorting private letters would require a disproportionate, unreasonable effort a

on behalf of the employer. However, the employer must justify this and make it necessary

to prove. In addition, the employer must provide adequate information on the operation of the system

employees, indicating to them, inter alia, the intervals at which they take place

backup on the system, thus assuring them, for example, that before the backup

they can actually delete their private correspondence.

However, as a legal basis for archiving the Applicant's e-mail accounts, the Debtor

indicated the employment contract concluded with the Applicant.

The grounds on which the processing of personal data may be lawful may be general

Article 6 (1) of the Data Protection Regulation. Although the general privacy

Article 88 of the Regulation is national in relation to employment-related data processing

within the framework set out in the provision

these national legislative measures shall be based on the legal bases set out in Article 6 (1)

may not be extended. Consequently, the controller is required to comply with Article 6 (1) of the General Data Protection Regulation.

may base its processing on one of the legal bases set out in points (a) to (f) of paragraph 1

in the absence of these conditions of legality - purely national

legal provision - is not sufficient to support the lawfulness of data processing, even then

nor if the General Data Protection Regulation itself concerns certain data protection legal bases

explicitly requires national legislative action.2

In the Authority 's view, the employment contract cannot be invoked as a legal basis because

so-called contractual within the meaning of Article 6 (1) (b) of the General Data Protection Regulation

legal basis may be used if the processing is necessary for the performance of the contract. The general

established under Article 29 of the Data Protection Directive3 in force prior to the Data Protection Regulation

The Working Party4 on the legitimate interests of the controller under Article 7 of Directive 95/46 / EC

6/2014 on the concept of 5 of the General Data Protection Regulation

may also serve as an interpretation during the period of application of the 2. 2.

that the contractual legal basis must be interpreted strictly. The legal basis is not applicable

situations where data processing is not actually necessary for the performance of the contract,

but it is unilaterally imposed on the data subject by the data controller.

It follows that, in the present case, the legal basis for the storage of archived e-mail accounts is a

The obligor may not rely on the employment contract as the performance of the contract on this

data management is not required.

However, this does not mean that the Debtor cannot have a legal basis for the Applicant's archive

to store your email accounts. Nor can that conclusion in itself necessarily be inferred from the fact that:

the controller in accordance with Article 6 (1) of the General Data Protection Regulation

based on a specific legal basis.

2

See, for example, Article 6 (3) of the General Data Protection Regulation.

On the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 95/46 / EC of the European Parliament and of the Council

3

Prior to the date of application of the General Data Protection Regulation, the Data Protection Working Party shall:

an independent European adviser on data protection and privacy issues

replaced by the European Data Protection Supervisor.

4

A 6/2014. Reviews can be found at the following link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

5

15

It should also be noted here, however, that it is in itself the data controller's data management

has not properly identified the legal basis for the processing, may necessarily lead to

laid down in provisions other than those laid down in Article 6 of the General Data Protection Regulation

failure to comply with the obligations incumbent on the controller or inadequate

and thus in relation to this breach in any of the general data protection regulations

to apply a specific legal sanction.

Based on the above, the legal basis for data processing in the case of bodies performing public tasks is the general one

may be the legal basis under Article 6 (1) (e) of the Data Protection Regulation, according to which a

the processing of personal data is lawful if the processing is in the public interest or to the data controller

in the exercise of a public authority conferred on it

required.

Since the disputed data processing is performed by the Debtor during the existence of the Applicant's legal relationship,

as a supplying body in order to comply with the rules of records management and information security,

storing e-mail accounts as a single database for a specified period of time

its need can be determined from the legal regulations and declarations. From this

consequently, the Debtor may have a legal basis for the entire archives of e-mail accounts

with regard to the processing of data relating to the preservation of personal data, including for both private and public

purposes

Article 6 (1) (e) of the General Data Protection Regulation.

Legal basis under point. However, this storage does not mean data retention indefinitely.

The opposite practice is the personal data in the single database

leads to purposeless, stock-based data management, which

and the principle of limited storage detailed in the following section. In addition, the

according to the records management rules, electronic documents related to work may not be stored in e-mail accounts, but in

an electronic file system in accordance with these rules,

or on paper, filed, as a record.

ARC. 2. 3. The principle of limited storage

It must therefore also be borne in mind that there is an unlimited retention period without indication of the period

leads to so-called inventory data management, which is contrary to the principle of limited storage.

This also follows from recital 39 of the General Data Protection Regulation, which states that

the storage of personal data may be limited to the shortest possible period of time and ensure this

In order to do so, the controller should have effective cancellation or periodic review deadlines

to establish.

However, the Debtor did not specify such deadlines in its IT security policy.

On the ordering of the MailStore archiving system available to the Authority

however, documents state that “there are no more lost emails” and “the MailStore

Server completely eliminates the risk of data loss ”. That is, the system - from it

Retains archived email content indefinitely, except for manual deletion

supported by the correspondence sent by the Debtor to the Applicant during the period under review

also containing stocks. This type of storage is contrary to the principle of limited storage
considered as data management. The circumstance relied on by the Debtor, according to which option
provided for the maintenance of the Applicant’s mailbox, a kind of for the Applicant
shall be assessed as an attenuating circumstance, however, in general it does not release the Debtor from the
from the obligation to cancel at regular intervals or from the fact that
stored indefinitely by the Applicant and, where applicable, by additional employees concerned
based on your system settings for the period under review. THE
Furthermore, according to the Debtor's statement, the Applicant has neither access nor influence over it
archives.

16

In view of the above, the Authority notes that the Applicant's private correspondence is a specific deadline
the Debtor has infringed Article 5 (1) of the General Data Protection Regulation by
the principle of limited storage in accordance with paragraph 1 (e).

ARC. 2. 4. Appropriate technical and organizational measures

In addition, as the Authority generally considers that employee and applicant e-mail accounts and
closely related to the archiving of their content is the appropriate regulation of them
and ensuring compliance with data protection requirements, he examined in this context
appropriate technical and organizational measures in accordance with the General Data Protection Regulation
compliance. Based on the information available to the Authority, during the period under review, 2018.
from 25 May 2018 to the date of the commencement of the official data protection proceedings.
the Debtor did not have internal regulations regarding the use of e-mail accounts and their content.
archiving. Regulation of data management in an internal document, the
recording of data management operations is necessary because from the planning of data management they are
all the essential steps taken to achieve the objectives, including the
the duration of data processing, the erasure or review of the processing of personal data
administration and documentation of the setting of deadlines, and at the same time

presupposes the ability to demonstrate compliance with data protection requirements. This principle a

in practice, inter alia, for data controllers in the General Data Protection Regulation

envisages the professional recording of regulations and procedures in accordance with the prescribed regulations. Appropriate

technical, organizational measures include built-in and default data protection

that the principles and data protection requirements are guaranteed

facilitated by the data controller.

In view of the fact that the Debtor had neither in fact nor at the regulatory level the

retention of the contents of e-mails, or no actual deletion, as well as regular

review deadlines in order to ensure that data protection principles are respected,

has not taken the necessary appropriate technical and organizational measures, in breach of

General Data Protection Regulation 24-25. both the Employees and the Applicant

with regard to.

In the opinion of the Authority, it is expedient for the Debtor to establish internal regulations a

rules for the use of email accounts provided to employees. The interior

These rules should cover, inter alia:

-

whether these e-mail accounts can be used for private purposes6,

-

backing up and storing and deactivating these e-mail accounts

and when emails will be permanently deleted,

-

detailed rules for checking and reviewing the use of e-mail accounts, who and

how you can exercise it within your organization, what your rights are

employee during the procedure.

The Mt. in force during the period under review did not contain any relevant rules, however, as of 26 April 2019

in force Mt. 11 / A. § (2), the employee is insured by the employer to perform the work

use a computer device solely for the purpose of performing an employment relationship - other agreement

in the absence of.

6

17

ARC. 2. 5. Responsibilities of the Data Controller of the Debtor

The Debtor argued that the Applicant was aware of the operation of the system because

he had previously ordered it as a leader. In the Authority 's view, in the light of this

the Applicant would also have been expected to assess the data protection aspects of the system.

It should be noted, however, that the Data Protection Working Party is the “data controller” and the

1/2010 on the concept of "data processor" in its Opinion No 7, in which the general

during the period of application of the Data Protection Regulation. 1.

(c) explained that for data processing, it follows from the data protection rules

the controller is responsible for these obligations. An exception to this is when it is clearly a natural one

a person’s liability can be established by the fact that in such a case, for example, when specific

a natural person is appointed to ensure compliance with data protection principles, that person

it will not be a controller but will act on behalf of the legal entity that is its controller

remains liable in the event of a breach of the principles.

Account must also be taken of the fact that the Applicant has not filled it for more than a year

the position of director when the archived contents of your e-mail accounts were checked, and that

others have already held this position during the period of general privacy

necessary measures have been taken to comply with this Regulation.

In particular, the Authority considers that, in order to avoid similar cases, it is appropriate to

if the employer informs the employees in detail about the archiving and its rules. THE

The Authority also considers it acceptable if, in the event of termination of employment, a

employer gives the employee concerned the opportunity to cancel for private purposes

emails from the email accounts he uses. In the Authority's view, this is a deletion

practicable on the last working day of the employee concerned by the employer,

the head of the employee's organizational unit or another person with decision-making authority in the organization

in the presence of an employee, avoiding the possibility of deleting documents where appropriate

which are not the employee’s private data. In the interests of legality, the Authority shall:

suggests keeping a record of this cancellation process. In the light of all this, the Authority considers that

the employer must draw up internal rules in order to comply with the principle of accountability

that he has taken all necessary measures to terminate the employment relationship

in order to protect the personal data of the data subject. If the employer has all these measures

nevertheless, the employee does not exercise his right of cancellation after the termination of the legal relationship is

reasonable

within the time limit and the employer can prove this, the employer shall not be liable. The Authority

also suggests that, if e-mail accounts can be used for private purposes,

in them, create a separate folder for private mail, excluding them for security

and, where applicable, after termination of employment

make it available to the data subject.

ARC. 3. Search e-mail archives containing private mail

ARC. 3. 1. Purpose and legal basis of data processing

For the purpose of searching the Applicant's archived e-mail accounts during the employment

referred to the finding of official documents in Article 11 of the Mt.

while relying on the employment relationship of the person concerned

marked an employment contract.

1/2010. Reviews can be found at the following link:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

7

18

The Authority recognizes the data processing purpose indicated by the Debtor as a suitable, legitimate data processing

purpose

as the documents necessary for the operation and work of the office, their mixing

the Debtor shall take all necessary steps to find

thus ensuring the continuity of work processes.

Regarding data management related to document retrieval in e-mail accounts a

Authority's position is that, like all data processing, in this case the Applicant is private

data management related to document searches in e-mail accounts containing e-mails

the Debtor must have an appropriate legal basis. In this case, the

The obligor had to comply with data protection requirements during his actions.

Annex IV to this Decision. 2. In view of the findings made in point 2, the Debtor relied on

The employment contract cannot be relied on as a legal basis for searching documents either, since

the legal basis under Article 6 (1) (b) of the General Data Protection Regulation is applicable when

if the data processing is necessary for the performance of the contract. In the present case, however,

data management related to document retrieval - also for termination of employment

is not necessary for the performance of the employment contract, so the Debtor is not entitled to this legal basis

can rely on.

However, as with storing archived email accounts, this does not mean that

the Debtor could not have had a legal basis in the Applicant's archived e-mail accounts,

work-related letters for search, as the public service

Due to its information security rules and statements, data management is in the public interest

necessary to carry out its tasks. Consequently, the Debtor

had a legal basis for working letters in the archives of e-mail accounts

with regard to the processing of personal data in connection with a search, which is covered by Article 6 of the General Data

Protection Regulation.

Legal basis under Article 1 (1) (e).

However, all of this can be found in the Applicant’s email accounts and is work-related only

applies to letters. To search the Applicant's private correspondence - as they are not

related to the employment relationship - the Debtor is not entitled to a lawful data processing purpose

and in the absence of an appropriate legal basis. Consequently, the Authority finds that the Debtor a

By searching your email accounts, which also contain your private mail

infringed Article 5 (1) (b) of the General Data Protection Regulation and the General

Article 6 of the Data Protection Regulation.

ARC. 3. 2. The requirement of fair data management

According to the Debtor 's statement, the search in the archives of the institution' s organizational and

by the Deputy Director-General in accordance with its rules of procedure, orally. According to the statement a

the search was made in a targeted manner, according to the subject of the sender and the letter, of which the Applicant was

not informed,

it was done in the capacity of an employer. For a search on the institution 's directorate - general, see

medical director and another staff member, as well as one from the institution's IT department

a staff member was present. However, the email you were looking for was not found in the archive, so it did not happen

document backup. In view of all this, the Applicant could not be present during the document search,

and thus there was no way of deleting, deleting, or deleting his letters for non-work purposes

make a copy for yourself.

19

Even if it is factually true that the email account is owned or controlled by the Debtor

therefore, you will be able to review it and search for a document in it without it

realize that it would require any intervention from the Applicant, this does not mean that

it would also be legal to review this type of email account and search for documents in it. On this

the principle of fair data management - the data management described above

due to the circumstances - there is also a requirement that during the review of the e-mail

as a general rule, the presence of the worker must be ensured. Fairness of data management a

the requirement of lawfulness, the right of the data subject to self - determination, and

through this it means respecting his or her privacy and human dignity: the person concerned does not

may become vulnerable to the controller or any other person. The data subject all the way

must remain subject to, and not become part of, the process of processing personal data

mere object. An email account review without an employee present is fundamentally the opposite of a

the principle of fair data management, as the intrusion into the employee's privacy

it counts as.

Informing the employee in advance and - in person or if this cannot be ensured -

proxy, presence - review your e-mail account and search for documents

also necessary because of the different personal data of the employee and third parties

may be included in the mail system, which are managed by the employer - personal data e

beyond the control of the nature of the If your email account is under review and document search

the employee - his representative, proxy - is present and may indicate any personal data

before viewing the contents of an e-mail that contains private e-mails

this ensures that the employer does not violate this prohibition.

However, depending on the circumstances of your e-mail account review, there may be situations where

when the personal presence of the worker cannot be ensured for objective reasons. The Authority shall:

therefore, in some exceptional cases, considers it acceptable that the

an employee is absent, for example in cases requiring immediate action, or a former employee

in case of. In this case, however, information must also be provided to the employee

on the other hand, the employer should be given the opportunity to:

he may not even be present, instead his proxy or representative shall be present. If this

preventive measures - prior information and the employee or his representative,

ensuring the presence of a representative - the employee is not available or does not appear

neither in person nor through a representative, in the absence of an independent third party

You can also access your email account to take immediate action

in order to. In this case, however, every effort must be made to ensure that the circumstances of the review of the e-mail

account are recorded in such a way that its exact course, the

the range of data learned in the process, ie the data management operations actually performed, and those

its legality can be verified ex post - also following the principle of accountability.

However, the Debtor did not meet these above requirements because, although stated in his statement

they searched the document purposefully, searching for the subject of the letter, did not take any action

in order for the Applicant to know in advance in their archived e-mail accounts

search for documents, or in order to be able to be present at that time

provide. In the opinion of the Authority, this behavior of the Debtor is data processing

violates the fairness of the applicant, as the Applicant thus did not have the opportunity to

to protect the personal data of other third parties involved in the correspondence

acting to indicate to the Debtor the private, personal nature of the letters. The Debtor is thus in control

without access to the Applicant - and, where applicable, third parties - for private purposes

correspondence. In the archived e-mail accounts of the Applicant without its knowledge

document retrieval is therefore contrary to the principle of fair data management.

20

Consequently, the Authority took steps to ensure the possibility of the Applicant's presence

due to the lack of steps, it finds that the data processing of the Debtor did not comply with the fair

breach of Article 5 (1) (a) of the General Data Protection Regulation.

point.

ARC. 3. 3. The requirement for adequate prior information and the principle of transparency

In order for data processing to be lawful and transparent, an additional requirement is that a

the employer must provide detailed information to the employees in advance

the possibility of reviewing the e-mail account in general, if any

review and search for documents, therefore the Authority also examined the existence of the information. THE

In the information provided, the employer must refer to Article 13 (1) to (2) of the General Data Protection Regulation.

the conditions for the processing of data pursuant to paragraph 1, paying particular attention to the fact that:

-

for what purpose and for what employer interests the email account may be reviewed

(Article 13 (1) (c) and (d) of the General Data Protection Regulation),

-

how the employer can carry out the review (general privacy policy)

Article 13 (1) (a) of the Regulation as the reviewer on behalf of the controller

representative),

-

the rules under which the data may be processed (compliance with the principle of gradation) and

the procedure (Article 13 (1) (c) of the General Data Protection Regulation),

-

what rights and remedies the employee has with the data processing

(Article 13 (2) (b) and (d) of the General Data Protection Regulation).

In addition to general information, information should preferably be provided prior to the specific action

employee about the interest of the employer in the data processing.

However, contrary to the above, the Debtor did not provide any information a

For the applicant on data management.

On the basis of all the above, the Authority concludes that the Debtor, as it did not provide in advance

a general overview of the Applicant's e-mail accounts in general and in a specific case, and a

information on data management and related information prior to document retrieval,

infringed Article 13 of the General Data Protection Regulation. Also given that the general

According to recital 60 of the Data Protection Regulation, it is transparent and referred to above

the principle of fair processing requires that the data subject be informed

and all information that is fair and transparent

necessary to ensure data management, a requirement which the Debtor has not complied with,

breach of transparency under Article 5 (1) (a) of the General Data Protection Regulation

principle as well.

ARC. 4. Accountability requirement

In the proceedings, the Debtor did not prove that the review of the Applicant's archived e-mail accounts
have taken any technical and organizational measures relating to data processing prior to the
including the storage of e-mail accounts as explained above. The Debtor is
justified the need for data management with regard to archiving and document retrieval,
however, it shall be diligent in accordance with the objective responsibility of the controller for the processing of the data
in breach of its data processing obligations
your data management. By doing so, he infringed Article 5 (2) of the General Data Protection Regulation.
principle of accountability set out in

ARC. 5. Sanctioning

The Authority examined of its own motion whether a data protection fine against the Debtor was justified.
imposition. In this context, the Authority referred to Article 83 (2) of the General Data Protection Regulation, Infotv.
Section 61 (4) (b) and Infotv. 75 / A. § considered the case all relevant
and found that the warning was issued in the event of an infringement being detected in the present proceedings
neither a disproportionate nor a dissuasive sanction, because during the storage of archived e-mail accounts that are the
subject of the request and document searches in them as data processing, the Debtor
has breached its obligations to a number of data controllers and a fine should therefore be imposed. THE
the specific preventive purpose of the Authority is to encourage the Debtor to
to carry out its data management activities consciously and not the data subjects as objects
treat them as genuinely entitled, ensuring their rights over the processing of their personal data
information and other conditions necessary for the exercise of control. And it is usually necessary
make it clear to all data controllers in a similar situation that personal data
handling requires increased awareness, there can be no such thing as relying on common sense in this area
to act without taking proactive measures, carelessly trusting that it will not come from

disadvantage of effectively uncontrolled processing of personal data. Such negligent behavior

it disregards the rights of those concerned and, as such, cannot go unpunished.

In setting the amount of the fine, the Authority took into account, in particular, that:

Infringements by the debtor within the meaning of Article 83 (5) (a) and (b) of the General Data Protection Regulation

(b) constitute an infringement in the higher category of fines.

The Authority took into account as an aggravating circumstance when setting the amount of the fine:

that the storage of archived e-mail accounts, including the Applicant’s private correspondence, is long

from the termination of the Applicant's employment relationship on 1 April 2017, which

from the date of application of the General Data Protection Regulation, 2018.

has taken into account the period starting on 25 May [Article 83 (2) of the General Data Protection Regulation

paragraph (a)].

The Authority took into account as an attenuating circumstance that

1. not to convict the Debtor for violating the General Data Protection Regulation

has taken place [Article 83 (2) (e) of the General Data Protection Regulation];

2. although for the data processing, for the obligations arising from the data protection rules, the Debtor

as data controller in charge, however, the Applicant as former director decided on the emails

the introduction of an archiving system, so that the characteristics of the system would have been expected of it

knowledge of [Article 83 (2) (k) of the General Data Protection Regulation];

3. upon the termination of the Applicant's employment relationship, he would have had the opportunity

maintain your mailboxes, delete your personal correspondence and personal data, taking into account

that he knew at least one month in advance that he would be terminated,

and you had access to your e-mail accounts for a month after your termination, so you could have taken steps to delete your

private mail during this period.

[Article 83 (2) (k) of the General Data Protection Regulation];

4. the Authority has exceeded the administrative deadline [Article 83 (2) of the General Data Protection Regulation

paragraph (k)].

The Authority also took into account that the data breaches found were intentional

in the absence of indications to the contrary, they are considered to be negligent [Article 83 of the General Data Protection Regulation.

Article 2 (2) (b)].

The Authority also took into account the special nature of personal data in deactivated e-mail accounts

categories were also found, however, with them the Required for Document Search was targeted

due to the nature of the data [Article 83 (2) of the General Data Protection Regulation

G point].

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

(j) as they cannot be interpreted in the context of the specific case.

The amount of the Debtor's own operating income according to the consolidated financial statements for 2018

it was in the order of HUF 1.3 billion. The data protection fine imposed is a token amount and does not enter into force

beyond the maximum fine that may be imposed.

In the course of the procedure, the Authority exceeded the Infotv. One hundred and twenty days in accordance with Section 60 / A (1)

administrative deadline, therefore Ákr. Pursuant to Section 51 b), it pays ten thousand forints to the Applicant.

V. Other issues:

The powers of the Authority shall be exercised in accordance with Infotv. Section 38 (2) and (2a) determine the jurisdiction of the country

covers the whole territory.

The decision is based on Ákr. 80-81. § and Infotv. It is based on Section 61 (1). The decision is based on Ákr. § 82

Shall become final upon its communication pursuant to paragraph 1. The Ákr. § 112 and § 116 (1),

or pursuant to Section 114 (1), there is an administrative action against the decision

redress.

***

The Ákr. Pursuant to Section 135 (1) (a), the debtor is entitled to the statutory interest rate

is obliged to pay a late payment allowance if it fails to meet its payment obligation on time.

The Civil Code. 6:48. § (1), in the case of a debt owed, the debtor is in arrears

valid on the first day of the calendar half-year affected by the delay

shall pay default interest at the same rate as the basic interest.

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) by decision of the Authority

The administrative lawsuit against the court falls within the jurisdiction of the court Section 13 (11)

the Metropolitan Court has exclusive jurisdiction. 2016 on Civil Procedure

CXXX. Act (hereinafter: Pp.) - the Kp. Applicable pursuant to Section 26 (1) - Section 72 provides for legal representation in a

case falling within the jurisdiction of the Tribunal. A Kp. Section 39 (6)

unless otherwise provided by law, the date of filing of the application

has no suspensory effect on the entry into force of an administrative act.

A Kp. Section 29 (1) and with this regard Pp. Applicable in accordance with § 604, electronic

CCXXII of 2015 on the general rules of public administration and trust services. Act (a

hereinafter referred to as the Customer's legal representative pursuant to Section 9 (1) (b) of the E-Administration Act

obliged to communicate electronically.

23

The time and place of the submission of the application is Section 39 (1). The trial

Information on the possibility of requesting the maintenance of the It is based on § 77 (1) - (2). THE

the amount of the fee for an administrative lawsuit in accordance with Act XCIII of 1990 on Fees. Act (hereinafter:

Itv.) 45 / A. § (1). From the advance payment of the fee, the Itv. Section 59 (1)

and Section 62 (1) (h) shall release the party initiating the proceedings.

If the Debtor fails to duly prove the fulfillment of the prescribed obligation, the Authority shall

considers that it has failed to fulfill its obligations within the prescribed period. The Ákr. According to § 132, if the Debtor

has not complied with an obligation contained in the final decision of the authority, it shall be enforceable. The Authority

decision of the Ákr. Pursuant to Section 82 (1), it becomes final with the communication. The Ákr. Section 133

enforcement, unless otherwise provided by law or government decree

ordering authority. The Ákr. Section 134 of the Enforcement - if law, government decree

or in the case of a municipal authority, a decree of a local government does not provide otherwise

carried out by a state tax authority. Infotv. Pursuant to Section 60 (7) in the decision of the Authority

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

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

implements.

Budapest, December 11, 2019

Dr. Attila Péterfalvi

President

c. professor