Case number: NAIH / 2019/769 /

(NAIH / 2018/5997 / H.)

Subject: Application in part

decision granting it

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

represented by […]; hereinafter referred to as "the Applicant", represented by […]; hereinafter:

Required) by reviewing the Applicant's email account and computing tools and

Data protection started on November 7, 2018

take the following decisions in official proceedings:

I. The Authority

IN ITS DECISION

1) the Applicant's request

and finds that the Debtor has acted in breach of the principle of fair data management in the

your personal information for reviewing and verifying your email account and for this

did not unlawfully provide prior information on control-related data processing;

2) the Authority instructs the Debtor to comply with the decision 15

review the Applicant's e-mail account during the review and verification of the aggrieved

not dependent (for private use) - you have known or stored your personal data and correspondence

annul the decision that, pending the expiry of the time-limit for bringing an action against that decision,

or, in the case of an administrative action, until the final decision of the court with the disputed data processing

the processing of the data concerned must be restricted in such a way that they cannot be deleted or not

may be destroyed, however, in storage and in administrative litigation by the court

may not be used otherwise than by use; in doing so, the Debtor is obliged to allow

make a copy of the data for personal use only for the Applicant 's own purposes, and

to duly inform the Applicant about the data processing in respect of undeleted data;

3) The Authority establishes ex officio that the Debtor, by checking the Applicant's e-mail account

in breach of the fundamental requirement of accountability

appropriate technical, organizational measures to ensure that it, the employees

in connection with the use of e-mail accounts and computer tools provided to

as well as ensuring the protection of personal data during its verification and did not take care

adequate information to stakeholders;

4) The Authority will instruct the Debtor ex officio to

within 30 days of the entry into force of this Regulation

ensure that workers take technical and organizational measures in accordance with

in connection with the use of e-mail accounts and computer tools provided to

protection of personal data, establish the necessary internal rules and

ensure that stakeholders are properly informed, including internal regulations for the control of e-mail accounts,

employees 'e-mail accounts by creating an appropriate prospectus,

control of its computer equipment.

2

5. The Authority shall reject the application in so far as it seeks a declaration that:

The Debtor unlawfully inspected the laptop and telephone provided to the Applicant.

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

within 15 days of the request of the Applicant, examine and inform the Applicant that

The laptop and telephone returned by the Applicant shall contain the personal data of the Applicant

and those for the management and termination of employment

no longer has a legitimate aim or legal basis, in particular

data processed for non-work purposes (private) - delete the present

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

pending a final decision by a court, the processing of such data shall be restricted in such a way as to

that they cannot be erased or destroyed, however, on storage and

may not be used in administrative proceedings other than by the court; of this

the Debtor is obliged to allow the use of the data for private purposes only for the Applicant's own purposes

make a copy and, in the case of undeleted data, the data processing to the Applicant

properly informed.

7) The Authority rejects the part of the application concerning the imposition of a data protection fine, however

Obliged ex officio

1,000,000, ie one million 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 / 2019/769 JUDGMENT. 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 shall fulfill the obligations provided for in items I. 2) I. 4) and I. 6) of this decision above

shall be in writing within 30 days of the date of notification of this decision

together with the submission of 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.

3

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. Facts, antecedents

I. 1. The Applicant submitted an application on 21 September 2018 through his legal representative a

To the authority in which he stated that he had been employed by the

However, with an obligation that terminated his employment with ordinary termination on July 18, 2018.

from the day. The Applicant complained that during the period of his incapacity for work due to illness

(in the days following May 23, 2018) in his absence from his desk and computer

accesses, devices, and e-mail account have been checked, the documents are physical

were relocated and photographs were taken of all these inspections, which

- in his view, resulted in unauthorized data processing and access. The Applicant requested it

the Authority, in order to establish an infringement, call on the controller to remedy the infringement,

or impose a fine if the conditions for an infringement are met. It also requested the Authority to:

prohibit the controller from handling, storing and storing personal data that has become available

transmission.

In its order to initiate the data protection authority procedure, the Authority notified the Debtor and

he called for a statement to clarify the facts.

I. 2. On the basis of the declarations of the Applicant and the Debtor and the documentary evidence attached by them, the

The period of incapacity for work due to the applicant's illness from 23 May 2018

On 25 May 2018, the Applicant telephoned his replacement staff and

specifically requested that he search the document on the Applicant 's desk and

take the necessary measures to deal with it. The Obliged - after the replacement

a number of outstanding documents based on the status of the document in question and the desk

found - in the absence of the Applicant - on the same day and then on 30 May 2018

his desk and the computer equipment in his office which is the property of the Debtor

scanned. The Debtor has access to some of these tools through work

related software, applications, systems, including in particular the Applicant's e-mail account […]. The Debtor also took

photographs of the inspection, which were later taken by one

Protocol dated 18 June 2018, and the Protocol based thereon, dated the same day,

also used to make a notice addressed to the Applicant. The email account in question is from Google Inc.

was a corporate email account created as part of a service provided by

the Debtor had the right to do so.

Although the Debtor disputes the fact of the inspection in a later statement made during the proceedings on 12 February 2019,

this is contradicted by the content of the attached protocol, the content of which is not disputed by the parties, the Applicant

and the Debtor

previous statements that the audit was established.

1

4

According to the Debtor's statement, an overview of the e-mail account and computer equipment,

During the audit, special attention was paid to the protection of personal data, therefore the phasing

following the principle, the sender and subject of the e-mail were examined first and then from a strategic point of view

e-mails deemed important were opened and immediate action was taken to avoid damage,
or mitigation. The audit is performed by an administrator and is called external
carried out by staff. The Chairman of the Director was also informed of the results of the audit. The Debtor a
has changed the password to access the email account in question, and
terminated for all documents available to the Applicant from the work server, or
access to the integrated corporate governance system it uses on a daily basis. The
After verification, the Applicant will no longer have access to your work email account
actively: he was still able to read his previous mail on his laptop, but his new incoming mail was already
he didn't see it, and he couldn't write an email using it.
At the instruction of the Debtor, the Applicant is the first to be absent due to incapacity for work
returned the telephone, which is also the property of the Debtor, to the Debtor on the business day of
laptop, which is stored on devices claimed by the Applicant, is detailed below
no personal data has been copied to or deleted from your device.
According to the Applicant's statement, he also used the information provided for his private purposes
computer equipment and your e-mail account, and therefore
and the data on the assets in its possession included the Applicant
Data, phone numbers, messages, and call lists needed to access your LinkedIn account
browsing history, web usage and location data. According to the Applicant's statement, a
a copy of the Applicant's identity documents (identity card,
address card), data recorded in connection with the use of the Internet, and for certain pages
usernames and passwords (such as the Bonus) and, in connection with the latter,
personal accounts and data content on a given page (such as the complete overhead of the entire household
account, turnover, payment details). Statement of the Applicant for this data
according to which the person could have accessed the device, so - the statement of the Applicant
for example, he may have been able to send a letter to anyone on his behalf or to enter the
personal LinkedIn profile. There was no evidence during the proceedings that the Debtor

would have actually had access to the data stored on the laptop or to the Authority in question

the exact data content of the media is unknown.

According to the Debtor's statement, he is not aware that the Applicant is personal on the devices

would have stored data and disputed that personal data had been disclosed during the above inspection.

According to the statement of the Applicant - not disputed by the Debtor - the Applicant was not informed

about reviewing your computing assets in your absence. You only received an smst on your business phone after you were

removed from your email account by changing your password.

Use of the e-mail account, laptop provided by the Debtor, or telephone

No written regulations or information were available from the Debtor. The Applicant

The private use of these devices was not prohibited. The Debtor, on the other hand

He referred to the Applicant orally, at the time of entering the job or at a management meeting

it was stated that it could not use the assets for private purposes, but beyond a mere statement

he did not support this.

The Applicant shall provide information on the inspection (documents in his office or on his office computer

had not been informed in advance, so that there was no way to

to copy your non-work personal information to your own device or to use it

delete, delete. Thus, in the absence of information in the minutes of termination

In the absence of any other document other than

the way in which it was carried out, the access to and possible storage of the data,

the rules and method used to verify the content of the e-mail account provided to you,

what happened to the return of data stored on your laptop and phone, how about your rights and redress

nor was he informed in advance of his options.

According to the Debtor 's statement, not primarily for audit purposes, but - originally a

At the express request of the applicant - the continuity of the duties of the outgoing staff member

access to the e-mail account and computer equipment was provided, and

they were inspected only due to the deficiencies detected during the replacement of the Applicant

May 25 and May 30, 2018. The Debtor shall take the integrity risk as the reason for this,

and indicated the economic interests of the Debtor, given the default of the Applicant

the Debtor was threatened with serious financial and legal consequences, the elimination of which, respectively

mitigation of its effects required the Debtor to take immediate action. THE

According to the debtor 's statement, the lawfulness of the review of the assets is also supported by the fact that

the assets and the e-mail account are the property of the Debtor and, as the owner, are entitled to them

the right to control.

The legal basis for the audit is the Debtor Act I of 2012 on the Labor Code (a

hereinafter: Mt.) § 8 (1), § 11 (1), § 17 (1) - (2), the

Act V of 2013 on the Civil Code (hereinafter: the Civil Code) 5:22. § and a

referred to certain points in his employment contract and his legitimate interest. The Debtor, however,

to prove that his legitimate interest took precedence over the interests of the employee and is fundamental

did not present to the Authority a formal prior assessment

balancing test.

The Debtor does not have internal regulations defining the detailed rules of workplace inspection

and there were no rules on the procedure for replacing employees

at will.

II. 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.

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

hereinafter: Infotv.) pursuant to Section 2 (2) of the General Data Protection Decree therein

shall apply with the additions set out in the provisions set out 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.

6

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 recital 39 in the preamble to the General Data Protection Regulation: '[t] he processing of personal data

above all, explicitly stated and legitimate, and

they must be specified at the time the personal data are collected. […] ”

Under Article 4 (1) of the General Data Protection Regulation: " personal data 'means 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 (2) of the General Data Protection Regulation: ““ processing ”means the processing of personal data

performed on data or files in an automated or non-automated manner

an operation or set of operations, such as collecting, recording, organizing, segmenting, storing,

transformation or alteration, query, insight, use, transmission of communication, distribution

or otherwise made available, through coordination or interconnection,

restriction, cancellation or destruction. "

According to Article 4 (7) of the General Data Protection Regulation, “data controller” means a natural or legal person

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 4 (10) of the General Data Protection Regulation: " third party 'means a natural or legal person

a legal person, public authority, agency or any other body which is not the same

with the data subject, the data controller, the data controller or the persons who are the data controller

or authorized to process personal data under the direct control of a data processor

they got."

Under Article 5 (1) (a) and (b) of the General Data Protection Regulation: 'Personal

data:

(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"). "

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) (b) and (f) of the General Data Protection Regulation: 'Personal data

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

(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;

(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 the Commission's decision on adequacy

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 24 of the General Data Protection Regulation: "1. The controller shall be the nature of the processing,

its scope, circumstances and purposes, and the rights and freedoms of natural persons

taking into account the reported risks of varying probability and severity

implement organizational measures to ensure and prove that personal

data shall be processed in accordance with this Regulation. These measures are taken by the data controller

review and, if necessary, update it.

2. If it is proportionate to the data processing activity, it shall be referred to in paragraph 1

As part of these measures, the controller shall also apply appropriate internal data protection rules.

3. For codes of conduct approved in accordance with Article 40 or approved in accordance with Article 42
joining a certification mechanism may be used as part of the demonstration that
the controller fulfills his obligations. "

According to Article 25 of the General Data Protection Regulation: “1. The controller is a science and technology
the nature, scope, circumstances and purposes of the data processing,
and the rights and freedoms of natural persons
taking into account the severity of the risk, both when determining the method of data processing and
and appropriate technical and organizational measures for data management, such as
pseudonymisation, which is based on data protection principles such as data protection
on the one hand, and the requirements of this Regulation, and the other
Incorporate the necessary safeguards into the data management process to protect the rights of data subjects.
2. The controller shall take appropriate technical and organizational measures to ensure that
that, by default, only personal data that is
necessary for a specific data processing purpose. This obligation applies to the collected
the amount of personal data, the extent of their processing, the duration of their storage and
their availability. These measures in particular need to ensure that you are personal
data cannot be changed by default without the intervention of the natural person
accessible to an indefinite number of persons.
3. An approved certification mechanism in accordance with Article 42 may be used to demonstrate this
that the controller complies with the requirements set out in paragraphs 1 and 2 of this Article. "

Under Article 58 (2) of the General Data Protection Regulation: 'The supervisory authority
acting in its corrective capacity:
(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 conditions laid down in 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. "

According to Article 83 (2) and (5) of the General Data Protection Regulation:

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).

[…] ”

In addition, Article 88 (1) and (2) of the General Data Protection Regulation provides:

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. "

Pursuant to Section 11 (1) - (2) of the Labor Code: “(1) The employer shall employ the employee only

in the context of his employment-related conduct. Employer control and

the means and methods used in the process must not violate human dignity.

The employee's privacy cannot be verified.

(2) The employer shall inform the employee in advance of the use of the technical equipment

for the control of the worker. "

According to Section 8 (1) of the Labor Code: “An employee during the existence of an employment relationship, unless

law, he may not engage in any conduct by which his employer has a legitimate economic interest

would jeopardize its interests. "

Pursuant to Section 17 (1) - (2) of the Labor Code: “(1) The employer shall §

in its internal rules laid down unilaterally or unilaterally

practice (hereinafter together: the employer's regulations).

(2) The employer's regulations shall be deemed to have been communicated if they are customary and generally known locally

published in an appropriate manner. "

The Civil Code. 5:22. §: “The owner has the right to use the thing and take the benefits of the thing;

bears the burden of the thing and the damage done to the thing for which no one is to compensate

may be required. "

III. Decision

III. 1. General remarks

According to the definitions in the General Data Protection Regulation, an e-mail account at work,

and the data content of the laptop or telephone provided to the employee is personal

any action taken on personal data shall be considered as data processing. From that

a separate issue is that personal data and data processing are limited to work,

is related to its purposes or is for private purposes for the benefit of the controller or the data subject

may be relevant in assessing the lawfulness of data processing.

In the present case, on the basis of the attached documents, it can be concluded that the Applicant is in use

the means provided by the Debtor, including the so-called ‘corporate e-mail account’.

including - used by the Applicant for private purposes.

In the case where an employee uses an email account, computer tools

- regardless of whether the employer otherwise prohibits or authorizes the private use

use - personal data stored in devices and systems provided by the employer

itself carries out data management activities.

11

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 the processing is, above all, the employment contract.

The data controller is the employer and the employee is concerned and the data is processed accordingly

to be judged.

However, in the case of an employee on assets provided by the employer and

also engages in private activities unrelated to the performance of work in the schemes and

in this connection, it handles the personal data of itself and, in most cases, other third parties, already

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

determined, but also by the employee, who may thereby become the data controller himself

in any way relating to the personal data of third parties

independent data management. He decides on the transfer of personal data to the system, device

and as long as the asset is in its possession, it may decide to cancel it,

other uses. However, with regard to this personal data, in particular “corporate

e-mail account ”, the operation and competence of the employer remains the operation of the system, and

nor does the employer who a

therefore remains a data controller for private data.

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

even if they appear without his express permission and unknowingly by him, by himself

systems used for specific data management in the context of other data management

personal data, on the one hand, they are persons who are actually acting in relation to their own data processing

they get there through. On the other hand, due to the circumstances of the data processing, it is actually possible

to process personal data in your system for purposes that it controls

they do not actually show any connection with data management2, their 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.

This conclusion is true even if the employer expressly excludes the assets for private use

as the nature of the data processing and the quality of the data processing are fundamentally a matter of fact (thus

the relevant provision can only lead to a different result on the issue of liability). Also in this

in the case of monitoring compliance with such a ban is actually the same data processing

operations, especially if the rule is not complied with, than if it did not do so

would be an employer. And in the case of the employee - a reasonable expectation only

if the employer also allows private use - it will explicitly inform the employer

What can almost never be ruled out in the case of a work email or mobile phone is provided as a work tool

and in the case of other computing devices, although it would be expected, it may occur in most cases

the employer is expected to count.

2

12

about the data for which the data is handled for private purposes

system / device, the employer's quality of data management only then does not appear

questionable if it can ensure the complete separation of such data processing a

from the processing of your personal data, including that you have no control over the personal data concerned

(for example, only the employee can decide on their storage and acquaintance)

In the absence of such complete separation, the employer shall in all cases be deemed to be the controller

pursuant to Article 4 (7) of the General Data Protection Regulation.

It should also be noted that as long as it is possible for the employee to have such, a

the processing of data stored solely for his own private purposes, ie for private purposes,

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 this. So it is his responsibility to recognize this situation and be proper

management of this with employer measures, so in the case of joint data management, data management

agreement on the details of the liability related to data processing

(essentially in accordance with Article 26 of the General Data Protection Regulation). Erre

even if the employer prohibits the assets it provides for private use

the control of this obligation and not this prohibition

in the case of suitable workers, this may in fact still be the case. That is something else

the question is whether the responsibility for data processing changes in such a situation,

as when data processing is implicitly or explicitly permitted.

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), the processing of such data will not be lawful, a

such personal data may not be processed by the employer. Unlawful data processing

primarily the general legal consequence is that the employer, as soon as it is informed of this

the fact of processing the data - terminates their processing, ie deletes them from its system, the

the means it provides. 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

13

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

to the most necessary circle to determine this quality of data and to control the process

be limited.3

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

who, in addition to using the device for work purposes, also for private purposes

uses the e-mail account and work tools 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.

In view of all this, it is advisable for the employer to draw up an internal regulation

rules for the use and control of e-mail accounts and computer equipment. With this

this is because it can prevent or reduce the possibility of workers (and

where applicable, the personal data of other data subjects involved in private correspondence)

employer. The internal rules shall cover, inter alia:

-

whether the e-mail account or computer device can be used for private purposes4,

-

backup of e-mail accounts, files on computer devices

to control the creation and storage of emails and when emails and files are permanently deleted,

-

detailed control over the use of e-mail account and computer tools

rules.

However, the prohibition of private correspondence or use in internal regulations is one

is an objective requirement for the staff of the data controller, but for the staff member

for third parties sending messages, with the exception of internal correspondence, shall not be covered by

the scope of the regulations, so at any time for private purposes, with the given work and activity of the employer

a letter containing unrelated personal information may be received by the employee electronically

to your mailbox.

The implementation of data processing - the general data protection regulation is personal data

not the subject-matter, official or private nature of the document, but its actual nature

the name, address, identifying details of the data subject and the procedure

other information provided in this document may occur in any document, including correspondence. In view of this, a

letters that are not private but specifically for work purposes also contain personal information.

Given that neither the data controller operating the system nor the user of the system

the nature of the content of the letter cannot in any event be delimited by the employee beyond a reasonable doubt

without examining the content of the correspondence, so it cannot be ruled out that the system is not alone

process personal data to the extent necessary and essential for the purpose of work.

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

processing on the part of him, if this is lawfully in accordance with Article 6 (1) of the General Data Protection Regulation

has a basis. However, such a permit alone is not enough, it requires a suitable worker

the details of such data processing are an actual agreement with the employee on a consensual basis

depending on whether you are cheating on the employee’s data or by third parties

whether it is also the processing of your data.

3

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

4

14

In case of violation of internal rules prohibiting private use - the employee in this regard

regardless of the reprehensible conduct of the employee - the employee and the third party are personal

data is actually processed, an objective situation occurs at the data controller

and the data processor used by him, thus creating a data management legal relationship, the

the resulting obligations shall be borne by the controller.

III. 2. Access to the email account provided to the employee

III. 2. 1. Purpose of data management

In the present case, two distinct objectives emerge: one is workflows

aimed at ensuring the continuity of the work of the absent worker

be visible, and as a result, your deputy will use your e-mail account for the duration of the replacement,

computer tools, to the extent necessary to perform the given task

and use documents. In this case, the performance of the employee to be replaced

they do not evaluate, they do not review which task, how they performed it, its purpose is simply to

absence of work processes due to absence.

In the case of the replacement of an absent worker, the replacement is typically another

provided by an employee to ensure the continuity of work that is required to perform the work

related tasks and also in view of the fact that the employer does not do so

- in addition to the continuous storage - a new data processing operation is personal to the employee

has no direct effect on the privacy of the employee to be replaced. In this

In this case, the employee's deputy appears as a performance assistant.

However, as in the present case, the failure to perform the duties

is documented and is subject to some form of accountability to the employee to be replaced

goes beyond the replacement and control of the work of the employee to be replaced

means.

This, which is separate from the purpose of replacement, is specifically derived from the employee's employment

personal data of the employee for the purpose of monitoring the fulfillment of his obligations

The essence of the activity associated with the treatment of

the employee’s e-mail account, computer equipment and

whether the task was performed by the employee and, if so, in what way. Of this

the end result is a certain level of evaluation and examination of the employee's performance,

how the employee has fulfilled his obligations arising from the employment relationship, which

it may also have employment consequences. This check must also comply with your privacy policy

requirements.

In the case of data management related to control, special attention should be paid to the purposeful

in addition to the principle of data management and the requirement of proportionality,

private, as there may be various non-employment personalities

data may also be disclosed to the employer or to persons not employed by him

you can also find out your personal information.

In the present case, the Debtor is subject to the integrity risk as well as the Debtor

economic interests, given that due to the Applicant's default, the Debtor

severe financial and legal consequences, the elimination of which or their effects

mitigation necessitated immediate action by the Debtor. The Authority on this

reasons, and the obligations of the Debtor as an employer pursuant to Section 11 (1) of the Labor Code.

recognized as a necessary and proportionate legitimate data management purpose by virtue of its right to control

verification of the Applicant. Consequently, the Debtor did not infringe in this respect

the provisions of the General Data Protection Regulation.

III. 2. 2. Legal basis for data processing

Pursuant to Section 42 (2) (a) of the Labor Code in force during the period under review, the employment contract
the employee is obliged to perform work under the direction of the employer. In line with this
the legislator as a fundamental duty of the employee in Section 52 (1) (b) and (c) of the Labor Code
specified that the employee is required to be at the disposal of the employer during his working hours
and his work with the expertise and diligence normally required for his work
according to rules, regulations, instructions and customs. In order to maintain these obligations
the legislator provides in Section 11 (1) of the Labor Code the possibility for the employer to a
check the employee for his or her employment-related behavior. This is the right
may necessarily involve the processing of personal data.

As the legal basis for the audit, the Debtor shall comply with Section 8 (1), Section 11 (1), and Article 17 of the Civil Code.
§ (1) - (2) of the Civil Code. 5:22. § as well as certain clauses in the employment contract and is legitimate
interest.

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 are set out in Article 6 (1)
may not be extended. Consequently, the controller is subject to Article 6 of the General Data Protection Regulation.
It may be based on one of the grounds set out in Article 1 (1) (a) to (f)
the lawfulness of the processing of personal data, failing which these conditions of lawfulness are met
a provision of national law - not to support the lawfulness of data processing
sufficient, even if the general data protection regulation itself is individual data protection
explicitly requires national legislative action on legal bases.5

The Civil Code. 5:22. In addition, the lawfulness of data processing cannot be considered to be the basis for the lawfulness of
data processing

as it relates to the use of property, the taking of benefits, the bearing of burdens in connection with the right of ownership and provides for exposure.

Section 8 (1) of the Labor Code, as indicated above, cannot be created independently either legal basis for data processing, as it contains the general requirement of conduct that a an employee may not, during the course of his employment, engage in conduct which: would jeopardize the legitimate economic interests of his employer.

Furthermore, § 17 (1) - (2) of the Labor Code cannot be applied as a legal basis for data processing either, as this provisions of the employer's regulations.

In the context of the employment contract as a legal basis, the Authority is also of the opinion that does not provide a legal basis for the management of data associated with the verification of e-mail accounts, as it is general established under Article 29 of the Data Protection Directive6 in force prior to the Data Protection Regulation

5

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

6

Data Protection Working Party7 6/2014. pursuant to Article 7 of Directive 95/46 / EC opinion on the concept of legitimate interests8, in which the General Data Protection Regulation was written may also be used as an interpretation during the period of application plea in law, in this case an employment contract, that that plea cannot be extended to interpret. The contractual legal basis does not apply to situations where the processing is in fact not necessary for the performance of the contract, but by the data controller unilaterally to the data subject it forces. Data management related to the verification of e-mail accounts is not in itself a case in point necessary for the performance of the contract of employment and is not the result of an agreement (especially if on-the-job inspection in the given workplace internal regulations, other than in accordance with the law

employment rule does not apply) and is therefore at issue in the present case

data processing cannot be based on an employment contract.

However, this does not mean that the Debtor did not have a legal basis to check the Applicant's e-mail account, nor can this

conclusion in itself necessarily be drawn from the fact that

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

based on a specific legal basis. As the Data Protection Working Party is a balancing act

test, but also in a way that is relevant to determining the appropriate legal basis

emphasized, “as with other vital aspects of data protection (such as the

identification of the controller or the purpose of the purpose), the statement of the controller

the reality behind it matters ”.9

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.

Data processing for the purpose of controlling the employee's work by the employer

The legal basis for data processing is Article 6 (1) (f) of the General Data Protection Regulation

may be the legal basis for a legitimate interest under which personal data in that case

can be managed if the data processing is necessary to enforce the legitimate interest of the data controller,

unless those interests take precedence over the interests or essential interests of the data subject

rights and freedoms that require the protection of personal data. As disputed

data processing is expressly permitted by the Mandatory Act, the Mt., in this way the legislator

legitimate interest recognized by the Commission, carried it out in the context of an employer's inspection and

legitimate access to the personal data required for this purpose

interest in the legislation and declarations and the supporting documents

means of proof (eg workplace inspection report and photographs) -

the Debtor has been threatened with serious financial and other legal consequences, the elimination of which, and

mitigation of its effects required the Debtor to take immediate action -

as a result.

In view of the information available to the Authority during the proceedings, the Applicant

no interests can be identified that would take precedence over the Debtor's legitimate interests

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.

7

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

8

9

A 6/2014. Opinion No III on Accountability and Transparency 3. Point 5 (page 47)

17

in the light of the information available to the Authority

The obligor complied with the principle of gradation during the inspection and no data were found that

that any personal data for private purposes beyond what is strictly necessary for the purpose of the inspection

would actually have been known.

In this context, however, the Authority considers it crucial to emphasize that

that in the present case the legal basis is Article 6 (1) (f) of the General Data Protection Regulation

on the basis of an assessment of all the specific and individual circumstances of the case, a

even in the absence of a detailed balancing test in advance laid down in writing by the controller

does not in any way follow that the controllers - the

Article 5 (2) of the General Data Protection Regulation, essentially the controller is objective

accountability, which sets out its responsibilities and due diligence

would not be liable for data processing on such a legal basis

the existence of the necessary conditions for the existence of a legal basis in advance and the processing of data

continuously monitored throughout its existence. And because it follows from the principle of accountability

proof that the conditions for the lawfulness of data processing are met at all times,

data controller’s responsibility, you can only trust any data controller to do everything

meets the legal requirements for data processing in this respect, if any

and the Authority, the court seised or, typically, the General Data Protection Regulation

In the event of the exercise of the right of objection provided for in Article 21, it shall also be sufficient for the person concerned

can demonstrate that these conditions are met. Beyond that, the specific legal basis

in the absence of the necessary discretion and documentation of the data controller

a number of obligations in relation to data processing (e.g.

ensuring the exercise of data subjects' rights, conducting data protection impact assessments

etc.) cannot be fully complied with, which could seriously infringe on the rights of those concerned,

and may result in a severe sanction accordingly. In view of the above, the Authority

considers it necessary to briefly summarize the expectations of this consideration.

According to Article 6 (1) (f) of the General Data Protection Regulation, it may then be lawful

data processing, where such processing is necessary for the legitimate interests of the controller, and

this interest is not preceded by any request for the protection of the personal data of the data subjects

interest or fundamental right and freedom. The controller therefore acts with due diligence when

if, for example, before carrying out data processing based on the legal basis of a legitimate interest,

6/2014 the balance of interests described in Opinion No

the data subject's own (or a third party's) legitimate interest and the counterparty to the weighting,

in cases such as the present - the interests of the employee, the fundamental right concerned, and only then

or continue to process the data if it determines, on the basis of the weighting of the two interests, the data subject

his own interests do not precede his own interests.10 In this consideration of interests, the case is always specific

on the basis of the facts and not in an abstract form, taking into account the reasonable expectations of those concerned

to act. The legal basis for a legitimate interest is generally applicable to the data subject to be enforced by the controller

(any) legitimate interest, but this general provision is explicitly ancillary

requires consideration to be given to the consideration of the controller or the data

the legitimate interests of the receiving third party or parties and the interests or fundamental rights of the data subjects.11

It follows from all this, as well as from recital 39 of the General Data Protection Regulation

with regard to the verification of e-mail accounts, the employer must have the data processing in advance

the e-mail account must have a well-defined data management purpose

to control. This goal (which is also the interest to be enforced is the most in line with this

10

A 6/2014. Article 7 (f): legitimate interests Point 3 (page 25)

11

A 6/2014. Opinion No IV Conclusions Point 1 (page 53)

the actual activity of the employer, the market situation and the

they must be appropriate to the job of the employees. In addition, the employer must

Before specifically verifying the use of an email account, you must tell employees that it is specific

in which case the employer's action is taken, as well as the right to protest

you must provide information.

Since, in accordance with the principles of proportionality and data protection, it is based on this legal basis

even in the case of data processing, only the processing of the data set absolutely necessary for the given purpose can be

lawful,

and whereas the scope, type and extent of data processed should be weighed in the balancing of interests

may also affect the weight of interests, 6/2014. In accordance with Opinion No

in accordance with the principle of gradual implementation, it is necessary to implement

and the balance of interests must be done in this way. In the case of such an approach, it is

only gradually become more difficult to intervene in the private sector concerned

In the case of data processing, personal data can be sufficiently enforced by providing appropriate guarantees

protection and the requirement that the inspection be kept to a minimum

workers 'privacy. For example, the first step in checking is your email address and letter

checking your subject may also be sufficient, as in some cases just the email address

It can also be seen from the structure and subject matter of the e-mail that it will be a private e-mail address and therefore

it is not necessary to know the content of the e-mail. This is especially important if a

employer allows employees to use a "corporate email account" in their internal policies

it is also used for personal purposes, as the employees then comply with the regulations

they may send or receive private e-mail to others. In addition, if

for example, your employer does not allow you to use your email account for private purposes and verification

it merely covers whether employees have complied with this by their employers

provision, it is also sufficient to view the email address and subject and not

it is necessary to know the content of the letter, since labor law consequences are already this fact

may also be applied to employees on the basis of

In connection with private e-mails, it is also necessary to emphasize the content of such e-mails

the employer is not, as a general rule, entitled to know, only for extremely compelling reasons,

in exceptional cases. According to the established data protection practice, the employer is ordinary

You are not authorized to review the contents of any private email stored in your email account

even if he informed the employees in advance of the fact of the inspection. The inspection

then the right of employees to the protection of their personal data and their right not to do so

the right of third-party employees to the protection of their personal data - and other

the right to privacy, in particular the right to privacy and the secrecy of correspondence, who

email was sent to or received from employees.

This can be done in more detail according to the next level of use of your email account

however, care should be taken here as well as the gradation and the information

are available to the employer in relation to the specific infringement, as they are

information may affect the focus and course of the audit.

However, given that the data disclosed in the present case are based on the Debtor’s above

in order to assert its legitimate interests, as set out in

limited to what is reasonably expected in the particular situation

continued its inspection and no evidence was provided that the data subject 's private sector,

would have covered the scope of non-work-related private data

inspection, the Authority considered that the general data protection was justified in all the circumstances of the case

the existence of a legal basis within the meaning of Article 6 (1) (f) of that Regulation. Regardless, however, the

It is obligatory to carry out the exact balance of interests described above

breached a number of guarantee rules of the General Data Protection Regulation

According to the following.

19

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

According to the Debtor's statement, since the e-mail account is owned by him, he can check it at any time

its contents. The Applicant was not informed about the inspection in advance, so this

in his absence, there was no way to be present at the inspection, not for work purposes

delete, delete or make a copy of your personal data.

Even if it is factually true that your email account and your work computer are the Debtor

is owned or controlled by it and can therefore control it without

that any intervention by the Applicant would be necessary does not mean that it is

such control would also be lawful. For data management related to workplace control

because of the principle of fair data management - the data processing conditions described above

As a result, there is a requirement that, as a general rule,

the presence of the worker must be ensured. The fairness of data management is also the legitimacy

the right of the data subject to self-determination, and through that

means respecting his or her privacy and human dignity: he or she cannot become one
vulnerable to the controller or any other person. The data subject is the subject throughout
it must remain a process involving the processing of personal data and not become a mere process
subject. Inspection without the presence of an employee is therefore fundamentally contrary to fairness
the principle of data management, as it treats the employee as a mere object, a manageable asset.
Informing the employee in advance and - in person or if this cannot be ensured -
his presence at the inspection is also necessary because the employee
and may contain different personal data of third parties in the mail system,
which the employer is not entitled to handle in addition to checking this nature of the personal data. If
during the inspection the employee - his / her representative, proxy - is present and can indicate
before viewing the content of an e-mail containing personal information for personal use
contains personal data, this will ensure that the employer does not violate this a
tilalmat.
However, depending on the circumstances of the audit, situations may arise in which a
the personal presence of the employee cannot be ensured for objective reasons. The Authority - as a general rule
otherwise, in some exceptional cases, it is therefore acceptable for the employee not to be present
present, for example in cases requiring immediate action, or a worker in sick condition
in case of urgent action. In this case, however, on the one hand, information
the employee must be given an opportunity about the planned employer action, on the other hand
he must also be assured that, even if he is unable to attend, you are his proxy instead
representative must be present at the inspection. If these preventive measures - preliminary
information and the presence of the worker or his agent,
however, the employee is not available or appears in person or as a representative
in the absence of an independent third party, your e-mail account, computer equipment may be accessed for
in order to implement it. In such a case, however, every effort must be made to
that the conditions of the inspection are recorded in such a way (where appropriate, the inspection

in the presence of persons not interested in the result as verifiers or otherwise

in an appropriate manner) that its exact course, the range of data learned during it, ie

the data processing operations actually carried out and their lawfulness can be subsequently verified,

also follows from the principle of accountability.

However, the Debtor did not comply with these requirements because he did not do anything

measure in order for the Applicant to become aware in advance of the

to ensure that he can be present at the inspection.

20

In the opinion of the Authority, this conduct of the Debtor is fairness of data processing

infringes, as the Applicant thus did not have the opportunity in his own - and, where appropriate, correspondence

to protect the personal data of other third parties concerned

The letters are private, personal in nature. The Debtor thus had access without control

to the personal data of the Applicant and, where applicable, third parties. The Applicant

an inspection that can be ordered at any time without the knowledge of the Debtor is therefore contrary

the principle of fair data management.

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.

III. 2. 4. 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 an audit in general, as well as before the specific review or audit, therefore the

The Authority also examined the existence of information on data processing ex officio. In the information a

employer must comply with Article 13 (1) to (2) of the General Data Protection Regulation

data processing conditions, with particular emphasis on:

- the purpose for which the e-mail account may be used and the interests of the employer, and

control of computer equipment (Article 13 (1) of the General Data Protection Regulation)

paragraph (c) and (d),

how the employer can carry out the inspection (general data protection law)

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

representative),

the rules under which inspections may be carried out (compliance with the principle of gradation) and what

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

- what rights and remedies the employee has in the e-mail account and

data management relating to the control of computer equipment

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

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

employee about the interest of the employer and the purpose for which the data is processed.

Contrary to the above, the Debtor did not provide any information to the Applicant

for data management.

On the basis of all the above, the Authority finds that the Debtor has not provided in advance

information on data management and related information, violated the general

Article 13 of the Data Protection Regulation. In addition, given the general data protection regulation

According to recital 60, transparent and fair data management as referred to above

principle requires that the data subject be informed of the fact and purposes of the processing, and

all information necessary to ensure fair and transparent data management

necessary, which requirement the Debtor did not meet, violated the general

Article 5 of the Data Protection Regulation. The principle of transparency referred to in paragraph 1 (a).

III. 2. 5. Appropriate technical and organizational measures

The Authority, as a general rule, employee and applicant email accounts and their general

closely related to the relevant regulations and data protection

to ensure compliance with the requirements, was examined ex officio in this context by the

21

appropriate technical and organizational measures in accordance with the General Data Protection Regulation

compliance with the Debtor. On the basis of the information available to the Authority, the

period - the Debtor did not have any internal regulations for the a

use of e-mail accounts, computing devices provided to employees, and

control of the data stored on these devices. Data management

regulation by the employer, recording of data management operations as appropriate technical,

organizational measure is necessary because from the planning of data management to its continuation a

all essential steps taken to achieve the objectives - including data management

deadlines for deletion and review of the processing of personal data

administration and documentation of the determination of the

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.

Although not regular, but immediate, ad hoc inspections, as in the present case, are not expected

that detailed internal rules be drawn up in advance for the specific case,

in any case, it is to be expected that such ad hoc inspections will be possible in advance

document and regulate how such inspections are to be carried out,

to whom the employee affected by the inspection may have access during a given inspection

computer equipment, e-mail accounts in order to

have clear information on their presence.

In view of the fact that the Debtor had neither actually nor at the level of regulations the

the use of e-mail accounts, the general and individual control of the content of e-mails

in order to ensure that data protection principles are respected

appropriate technical and organizational measures, infringed Article 2425 of the General Data Protection Regulation for both

employees and the Applicant.

III. 3. Verification on the laptop and telephone provided to the Applicant

rejection of the application for a declaration of illegality

The Authority shall reject the part of the application seeking a declaration from the Authority that:

The Debtor unlawfully checked the laptop and telephone provided to the Applicant,

as no information was provided that the Debtor actually had access to this

personal data of the Applicant.

However - in view of the fact that the data carriers in question are disclosed in the Debtor

the Authority held of its own motion the data stored on the media in question

the need to settle his fate in accordance with the general data protection regulation.

III. 4. Accountability requirement

The Debtor in the proceedings did not prove the verification of the Applicant's e-mail account

have taken any technical and organizational measures relating to data processing prior to the

including the prior balancing of interests as set out above. THE

The debtor has identified a legitimate interest in the particular data processing in the present proceedings

the need was also justified, however, the data controller wore an objective for data management

by failing to fulfill its obligations arising from the careful handling of data in accordance with its responsibilities

implemented your data in an infringing manner. With this behavior he violated the general

accountability as defined in Article 5 (2) of the Data Protection Regulation

requirement.

III. 5. Sanctioning

The Authority rejected the Applicant's application for a fine, as e

the application of a legal sanction does not directly affect the right or legitimate interest of the Applicant,

such a decision of the Authority shall not create any right or obligation for it

As regards the application of a sanction falling within the scope of the public interest,

with regard to the imposition of fines, the Applicant shall not be considered a customer in accordance with Ákr. Section 10 (1)

or, as the Acre. Does not comply with Section 35 (1), application in this regard

this part of the application shall not be construed as an application.

However, the Authority examined of its own motion whether it was justified against the Debtor

imposition of a data protection fine. In this context, the Authority shall, in accordance with Article 83 (2) of the General Data

Protection Regulation,

and Infotv. 75 / A. § considered all the relevant circumstances of the case and

found that no warning had been given in respect of the infringement found in the present proceedings

is a proportionate and non - dissuasive sanction because the individual control that is the subject of the request is

in the course of data management, the Debtor has breached its obligations to essentially all data controllers,

and in relation to work-related data management in general during the disclosed facts

has therefore failed to fulfill its obligations under the General Data Protection Regulation by imposing a fine

required. By imposing fines, the Authority 's specific deterrent effect is to encourage

It is obligated to continue its data management activities consciously and not to the data subjects

as a rightholder, ensuring that their rights and data

information and other conditions necessary for the exercise of control. And usually

it is necessary to make clear to all controllers in a similar situation that

the processing of personal data requires increased awareness, it is not possible to use common sense in this area

to act without taking any proactive measures, negligently

that there is no disadvantage in the actual uncontrolled processing of personal data. That's it

negligent conduct completely disregards the rights of those concerned and, as such,

it essentially undermines their human dignity and, as such, cannot go unpunished.

In determining the amount of the fine, the Authority took into account that the Debtor

Infringements under Article 83 (5) (b) of the General Data Protection Regulation a

constitute a higher category of fines.

The Authority also took into account the following relevant factors when setting the amount of the fine

take into account:

-

as an aggravating circumstance that the Debtor is the victim of the rights due to the infringing conduct

significantly hampered the exercise of

-

the Default of the Debtor is not considered to be expressly intentional, but serious

is considered negligent

-

as a mitigating circumstance that you are obliged to be convicted under the General Data Protection Regulation

has not yet taken place due to a breach of

-

as an attenuating circumstance that the inspection as an immediate measure, the Debtor

necessary to prevent or mitigate imminent

23

-

as an attenuating circumstance that, on the basis of the information available to the Authority, the Debtor

not sensitive information about the Applicant's privacy during the inspection

got to know

-

As a further mitigating circumstance, the Applicant itself may have made a significant contribution to

that on the devices made available to you for work purposes, in an e-mail account for that purpose

data processing for incompatible purposes could take place without being stored for a different purpose

personal data would have been easily separable.

The net sales of the Debtor in 2018 were HUF 1,651.94 million, so the data protection fine imposed

does not exceed 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.

ARC. 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.

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:

24

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

implementation, 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, the decree of the local government does not provide otherwise - the

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, October 15, 2019

Dr. Attila Péterfalvi

President

c. professor