Case number: NAIH / 2019/5062/5

dr. For Ákos Ányos Hadházy

parliamentarian

Budapest

Széchenyi quay 19.

1358

Dear Sir,

As reported by the National Data Protection and Freedom of Information Authority (hereinafter: the Authority)

previously informed, a notification was received by the Authority in which the petitioner dr. Ákos Hadházy

Ányos Member of Parliament (1358 Budapest, Széchenyi Quay 19; e-mail:

hadhazy.akos@parlament.hu; hereinafter referred to as the "Data Controller") to the European Public Prosecutor's Office

objected to the processing of his data relating to the collection of signatures

The Authority was thanked for receiving NAIH / 2019/5062/2. related to case number issues

information.

(A) At the request of the Authority, you have informed the Authority of:

1. The Data Controller shall provide the full names, addresses and, optionally, the data subjects in connection with the

collection of signatures

manages your email address and phone number.

2. The full names, addresses, e-mail addresses and contact details of the data subject

telephone number on the basis of consent.

The data provided in the event that the data subject provided e-mail and / or telephone

contact details until the data subject's consent is withdrawn, if not

provided data for contact purposes, data after completion of collection (30 May 2019) 3

treats for months.

3. The Data Controller shall transfer the personal data provided by the data subjects to the European Public Prosecutor's

Office

telephone and / or e-mail availability

intended to use the authorization for political contacts.

The data may be disclosed to the employees or to the natural and legal persons to whom it relates

Data controller for political communication or IT tasks in the form of a contract

trustee.

Storage of data in physical form (paper, handwriting) before deletion, 24-hour security service,

under the supervision of a fire alarm system and a camera system in a multiple enclosure.

After processing, the data is currently stored in a spreadsheet (.csv) format in Mailchimp

the Data Manager also backs up Sync.com in .csv format.

4. Notarization would have taken place when the 1 million signatures were reached. THE

authentication of contact information is personal based on the information provided for contact

during contact with proof of identity. Consent to contact

data from non-taxable stakeholders were randomly checked.

No contract was concluded with a notary, therefore no data processing was carried out by a notary.

5. Stores the address, telephone number, e-mail address and full name of the data subject as "contact details"

the Data Controller.

For the contact, the name and address to provide personal, territorially relevant information

serves as the email address for written documents and messages to the general public at the same time



the phone number is for personal, urgent, or near-time events

information and access for citizens without a computer. You do it

stated that they all meet the purpose of data management, communication, and help

compliance with the requirement of accuracy and up-to-dateness, since if one of the data

If it turns out to be unreadable or incorrect, you can request another contact method

correction, or the ability to enter multiple types of contact information for custom modes

allow the controller to adapt to his preferences.

Storing personal information in your Mailchimp system that is treated as "contact information" .csv
format on Sync.com in .csv format. The storage of paper sheets is
24-hour security service, fire alarm system and camera system monitoring until destruction
takes place several times in a closed place.
6. As stated by the Data Controller, you are the only user of the databases
experts with a data processing contract are essential for the maintenance of
staff has access with multi-factor authentication, so access is not currently logged. The
personal data provided by data subjects through encrypted channels for security data transmission
They are transmitted to the Data Controller protected by the SSL web protocol and forwarded to the Data Controller's
newsletter or cloud service provider. Special security programs are used and regular security
inspections are carried out. In addition, the Data Controller states that it is a trusted server provider
uses where outbound connections are logged to track any intrusions. THE
they use the latest technology and perform regular backups.
Outside Hungary, only with a secure and adequate level of data protection and certification
GDPR compliant services in the third country with a mechanism (US: EU-US
Privacy Shield, Canada). The use of data overwriting and backup peripherals is severely restricted, as such
protects your data with encryption. Data and media no longer needed are supervised by 2 witnesses
destroy it.
7. When uploading the completed signature collection forms at https://europaiugyeszsegert.hu/feltoltes/
legal basis for the management of a mandatory e-mail address or telephone number - data management
as set out in the prospectus - the consent of the data subject. The purpose of data management is a
contact, including clarification of data resulting from incorrect or illegible uploads; and
requests for rectification. This data is stored by the Data Controller until the consent of the data subject is revoked
handles.
The duration of data processing has been clarified in the data management information: a
For the sake of clarity, all links to the Internet

according to the content of the text in the contact or data management information checkboxos

entering a consent field until the consent for the data provided has been withdrawn

consent to its treatment. These fields have previously pointed to this prospectus and

data processing was allowed until the withdrawal of consent, but more precise and clear

their name has changed for information purposes, which is not the case in the data management information notice

followed immediately.

8. Political parties with the same issue, but as separate data controllers, own, separate

participated in the collection with data management information. Regarding the collection of signatures of the parties, the Data Controller

He has no written contracts and no data controller authority, therefore

cannot provide details.

9. Data collection lasted from 19 July 2018 and from pre-registration to 30 May 2019. The registration and

upload surfaces have been closed.

10. The Data Controller has attached the contracts concluded with the data processors used during the data processing

copies.

3

B) After reviewing what was written in its response letter, the Authority took the following position on the matter

developed by:

I. The Data Controller is entitled "Join the European Public Prosecutor's Office!" initiative called

collected the following personal data of the data subjects in the support sheet: name, address (postcode,

city, address), e-mail contact, phone number, signature.

Name, signature, address, e-mail contact and telephone number according to GDPR definitions

the personal data of the data subject1, any operation performed on the data, such as data

collection, recording and storage is considered as data management2.

Under the provisions of the GDPR, a number of requirements must be met for the lawfulness of data processing.

Of these, the legality of Article 5 (1) (a) and (b) of the GDPR plays a key role,

the principles of fair trial and transparency and purpose. In addition, the

the controller must have a legal basis in accordance with Article 6 (1) of the GDPR

for data management.

Article 9 of the GDPR also provides for the processing of special categories of personal data. These

personal data referring to a political opinion, the processing of which is regulated by the Regulation

prohibits it as a general rule or makes it subject to strict conditions. This special category is personal

data may be processed, inter alia, only with the express consent of the data subject

for one or more specific purposes.

In its reply to the Authority, the Data Controller indicated the consent of the data subjects

as the legal basis for data management, as well as in the Privacy Statement on the back of the sheet

refers to the consent of the parties concerned.

Pursuant to Article 6 (1) (a) of the GDPR, the processing of personal data is lawful if it

the data subject has consented to the processing of his or her personal data for one or more specific purposes.

Article 4 (11) of the GDPR states that the data subject consents to the will of the data subject

voluntary, specific and well-informed and clear statement by the data subject

by means of a statement or an act which unequivocally expresses its confirmation

for the processing of personal data concerning him.

The data collection page of the sheet contains the following information: “Data Management Information -

I accept the prospectus with my signature ”, while the text of the Privacy Notice on the back of the sheet

“The legal basis for data processing is clear after reading this information

consent. ".

In order for the controller to be able to legitimately invoke the legal basis of the consent, the consent

all its conceptual elements must meet the requirements that apply to it.

The Working Party on Data Protection set up under Article 29 of the Data Protection Directive

Guideline WP259 also explains whether the statement or confirmation

an unequivocally expressive act is a precondition for regular consent. Expressed to the person concerned

GDPR Article 4 (1): "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); identifiable

a natural person who, directly or indirectly, in particular by means of an identifier such as name, number, location data, online identifier

or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person

identifiable by.

2

Article 4 (2) of the GDPR: "data processing" means any operation, whether automated or non-automated, on personal data or files

or a set of operations, such as collecting, recording, organizing, sorting, storing, transforming or altering, querying, accessing, using,

by transmission, distribution or otherwise making available, coordination or interconnection, restriction, deletion or destruction. "

Article 4 (7) of the GDPR: “controller” means any natural or legal person, public authority, agency or any other body which determine the purposes and means of data processing, either individually or in association with others; if the purposes and means of the processing are governed by Union or Member State law

the controller or the specific criteria for the designation of the controller may be determined by Union or Member State law. "

1

4

you must make a statement of consent. Belief that the consent is explicit

an obvious way would be to explicitly confirm the consent in a written statement. To

it is therefore necessary for the data subject to be able to express his or her will in concrete terms

information related to obtaining consent for data management activities

clearly separate it from information on other issues.

Recital 42 of the GDPR also states that it is pre-formulated for the controller

provide a statement of consent in a comprehensible and easily accessible form

and its language should be clear and unambiguous and not

may contain unfair terms.

In the Authority's view, it is only that the data subject provides the requested form on the signature collection form

shall not be considered as a specific, unambiguous expression of the will of the data subject and

The “acceptance” of a privacy statement with a signature is not considered personal data either

unequivocal expression of the consent to the use of

The data subject does not have to "accept" the prospectus, but needs to process the data on the basis of the information

consent to the processing. THE

the consent is therefore closely linked to the information, as the data subject is the relevant information

in his possession, he may decide whether to give his consent to the personal data concerning him

to treat. In relation to the information, the data subject may be expected to make a statement

that it has become acquainted with its contents, has taken note of its contents, and its role is therefore limited to

that he can prove that the consent is informed.

Consent by giving it as explained above is not

clear and concrete expression of the will of the data subjects, data processing is not considered

without a valid legal basis, the Data Controller shall handle the personal data of the data subjects

in breach of Article 6 of the GDPR. Because this information is personal information is special

categories and may be dealt with, inter alia, in the case of

to the controller, with the express consent of the data subject, the processing infringes Article 9 of the GDPR.

Article 1 (1).

II. Article 5 (1) (b) of the GDPR provides for the principle of purposeful data processing, according to which

personal data may only be collected for specified, explicit and legitimate purposes and used for such purposes

they may not be treated in a way incompatible with those purposes.

II.1. According to the Privacy Policy of the sheet, the purpose of data processing is the name, address and signature

the collection of supporting signatures and their joint voters

submission to the notary. If contact information (phone number,

e-mail address) has also been provided, according to the Privacy Notice, all data - the telephone number

and / or e-mail address, the purpose of the name, address and signature is to enable the controller to

in connection with the activities of members of parliament

contact information.

In its reply to the Authority, the Data Controller stated in this regard that

collected the data of the data subjects in order to facilitate the accession to the European Public Prosecutor's Office and with

the notary

authentication would have taken place when the 1 million signatures were reached.

Regarding the purpose of the data processing, he also stated that the data of the data subjects,

if authorized by providing telephone and / or e-mail contact details,

used for political communication.

In the course of the investigation, the Authority found that the data collection side of the sheet was for each

there was no specific indication or call for the personal data to be collected

the provision of data is mandatory for the validity of the initiative's support, or the provision of information



optional and for collection for other data management purposes other than in support of the initiative - present

in this case for contact purposes.

Provide telephone and / or e-mail contact details on the signature collection form, taking into account that the

there is no specific notice that the provision of this information is not mandatory - it is not considered

on the one hand, confirmation of consent to the use of personal data

unequivocally expressive act and, on the other hand, cannot be

consent to the processing of personal data for contact purposes.

Recital 32 of the GDPR states that where data processing serves several purposes at the same time,

then the consent must be given separately for all data processing purposes. If it is

the controller does not attempt to request consent for each purpose separately, a

freedom of choice.

In the Authority's view, the lawfulness of the processing of the personal data of the data subjects at that time

can be established if the data subject is used for all data processing purposes

may have contributed separately to its treatment.

II.2. During the period of signature collection, it was possible to complete the completed signature collection forms a

Also for uploading via https://europaiugyeszseget.hu/feltoltes/. During charging, respectively

the following personal data was required for its successful completion: name

(surname and first name), e-mail address, county, town, telephone, and were required

Adoption of data management information. Data management is included in the Data Management Information

The aim is to contact and liaise with supporters of the European Public Prosecutor 's Office

stakeholders

the

European

Prosecution

supportive

activities

about events

notifications of movements and signatures.

In the response of the Data Controller to the Authority, the data subjects are the legal basis for the data processing

and the purpose of the data processing is to keep in touch and to ensure that the

You can also use the contact information provided to make it incorrect or unreadable

request clarification and correction of the data resulting from the uploads.

It can therefore be concluded that in order to handle the personal data provided when uploading the forms online, the

their consent has been given by those concerned as indicated above, subject to mandatory completion

fields, enter your personal information and the checkbox next to the Privacy Notice

marked. It was therefore not possible to fill in the sheet as long as the requested personal data a

the uploader did not enter or checkbox.

According to Article 4 (11) of the GDPR, one of the most important elements of a valid consent is

volunteering.

In this respect, recital (42) of the GDPR states that consent is given

shall not be considered voluntary if the person concerned does not have a real or free choice,

and shall not be able to refuse or withdraw consent without prejudice. THE

Furthermore, as stated in recital (43), the consent cannot be considered voluntary if

it does not allow separate contributions to different data management operations, although that is the case

appropriate in this case.

The Data Protection Working Party in its Guidance on Consent WP259 on a voluntary basis

with regard to a given contribution, found that the “free” element presupposes that the

those concerned have a real choice and right of disposal. As a general rule, the GDPR

provides that if the data subject does not have a real choice, he is forced to give consent

you feel or you will have negative consequences if you do not give your consent, then your consent

not valid.

The Authority found that the provision of data during the online upload of the forms could not be considered

at the same time, the consent of the data subject to the processing of his or her data for the purposes of contact



without providing the data, ie in case of refusal of consent

there was an opportunity for the data subject to complete the signature collection form through the site.

The lawfulness of data processing requires a separate, valid legal basis for all independent purposes

both to support the initiative and to liaise

for data processing purposes. Stakeholders for all data processing purposes

As explained above, the main conceptual elements

which are necessary for the consent, ie the legal basis for the processing, to be valid

be. There is a lack of voluntary, specific, well - informed and

a clear statement by which you consent to the processing of your personal data.

In the Authority's view, therefore, the Data Controller treats the data subjects without a valid legal basis

personal data, both during the data collection in the signature collection form and in the

data collection for contact purposes, in breach of Article 6 of the GDPR. Because

these data fall into special categories of personal data and their processing

among other things, the controller has the option if the data subject has expressly requested to do so

data processing also infringes Article 9 (1) of the GDPR.

III. An important conceptual element of a valid consent is that the request for consent is properly communicated

prevent it. Adequate prior information is needed to keep those concerned informed

be specific to what they agree to know the details of the data management and

exercise their right to withdraw their consent. Failing this, the consent

that is, the legal basis for data processing will be invalid.

Article 5 (1) (a) and (b) of the GDPR and, in this context, Article 39

Recital 1 also states that it should be transparent to natural persons

be how their personal data about them is collected, used, in that

considered or otherwise treated, and in the context of being personal

the extent to which data is and will be handled. The principle of transparency applies to those concerned

also for the purposes of data processing. The specific purposes of personal data processing are explicit

and lawful, as well as the collection of personal data

must be specified at the time of

Article 13 of the GDPR defines what information is available to data subjects

shall be informed at the time the data are obtained.

III.1. Information on the conditions of data management in the signature collection form

In its investigation, the Authority found that the data processing of the signature collection form

As explained above, the Data Controller did not inform the data subjects in the prospectus

the legal basis and purpose of the processing.

As regards the identification of the recipients of personal data, the Authority has established that

In the data management prospectus, the data subjects were informed that the Data Controller is the signature collector

will be submitted to a notary public no later than 31 May 2019, so that the collected supporting signatures

regardless of the number. At the request of the Authority, on the other hand, the Data Controller stated that a

notarization would have taken place when the 1 million signatures were reached, and given that

the required number of supporting signatures was not collected and no contract was concluded

notary, so there was no data processing by a notary. In the Authority 's view,

information on the recipients would therefore have been complete if the parties had been informed

that the sheets and the personal data contained therein were notarized

will be handed over only if the appropriate number of signatures is collected, or

they would have been informed of what would have happened after the submission to the notary

sheets and thus the personal data on it. In the prospectus therefore

nor was there any information on what would happen to the arches if a sufficient number of signatures were collected

and all personal data contained therein.



In its reply to the Authority, the Data Controller provided information on the data used

data processors, however, in the Data Protection Bulletin attached to the sheet, the data processors

those concerned were not informed of its use. Stakeholders were also not informed that

whether or not the activists commissioned by the Data Controller qualify as data processors. It is not clear

and who is to be understood as the staff of the Data Controller or the ‘staff’ do not know whether the

What is the legal relationship of the data controller with these persons, who perform the tasks of data management

during.

Regarding the duration of the storage of personal data collected in support of the initiative,

The privacy statement contained only the information that the signature collection forms were notarized

after submitting the data to the notary for consideration of the petition initiative

must be deleted after. However, there was no information as to where the arches were

however, they will not be filed with the notary when they are canceled.

The Authority has established that, on the basis of the above, the Data Controller -

in the Data Management Information Sheet of the Signature Collection Form - did not provide information to the data subject

all relevant circumstances of the data processing, in breach of Article 13 of the GDPR

included.

III.2. Information on how to handle the information you provide when uploading forms online

The legal basis and purpose of the processing of personal data to be provided during the online upload

In relation to this information, the Authority noted that it had provided the Data Management Authority

as stated in the Privacy Policy linked on the Upload page

the legal basis is the consent - they contradict the actual content of the Data Management Information, a

The legal basis of the data processing has not been indicated in the prospectus, it is only informed by the

stakeholders what they consider to be the purpose of the data processing.

The Authority shall provide information on the duration of the processing during the investigation

found that, as stated in the prospectus, it was provided when uploading the forms online

personal data will be processed until the end of the signature collection operation, but with a specific date for this

was not indicated, so it is not clear to those concerned that their data will be

How long the data controller will handle it.

According to the prospectus, further provided on the form with the Data Controller's political activity

the newsletter has been subscribed, the data will be processed until the consent is withdrawn. THE

Authority in the course of the investigation found that the online upload must be a mandatory form

there was no possibility to subscribe to the newsletter, therefore uploading the forms online

at the same time it could mean subscribing to the newsletter, for which purpose the data subjects

they could not give their consent separately.

During the investigation, the Authority found that https://europaiugyeszseget.hu/adatkezelesi-tajekoztato/

available in the Data Management Information on the website several times - on July 16, 2019

and 31 August 2019, of which the amendment of 16 July 2019 was amended by

The data controller also provided information in his reply to the Authority. However, these changes

on the one hand, they took place after the examined data management period, and on the other hand, no changes with such

content were made

which would have changed the Authority's findings.

The Data Controller did not provide clear, adequate information to the data subjects during the period under review

and real information provided by the personal information provided when uploading the forms through the website

all relevant circumstances of the processing of personal data, thereby infringing Article 5 (1) of the GDPR.

Article 5 (2) and Article 13 (1) to (2).

8

ARC. Validity of the legal basis for data processing

According to the definition in Article 4 (11) of the GDPR, the data subject's consent is the data subject

voluntary, specific and well-informed and unambiguous declaration of will,

by which the statement concerned or the act of confirmation is unequivocally expressed,

to give his or her consent to the processing of personal data concerning him or her. So consent then

considered as a valid legal basis for data processing if all the conditions are met.

One of the most important components of the validity of the consent is the voluntary nature of the will of the data subject,

freedom from outside influence, which is achieved when there is a real choice

available to the person concerned. Where the consequences of consent undermine an individual's election

consent is not considered voluntary and is therefore a valid contribution.

A specific, clear, unequivocal statement or affirmation of the will of the data subject

the requirement to disclose by act means, on the one hand, that consent

on the other hand, clear, explicit consent is also a goal

also consent: can be considered as consent for a specific, specific data processing purpose.

As a general rule, the data may not be used for other data management purposes.

All conceptual elements of consent can be fully valid if the consent is requested

preceded by appropriate information. The right information is through which stakeholders are involved

they are familiar with the processing of their personal data and are able to do so through the information

the right to self-determination of information is enforceable: the processing of data may be lawful under the circumstances

they are fully known to those concerned. The requirement to inform the data subject in advance a

Article 13 of the GDPR details this.

In the opinion of the Authority, the above I., II. and III. as a result of the above

its contribution to data management lacks the most important conceptual elements that

necessary to provide the legal basis for the processing, in this case consent

be valid. The Data Controller handles the personal data of the data subjects without a valid legal basis,

in breach of Article 6 of the GDPR.

V. Pursuant to Article 28 (1) of the GDPR, if the processing is carried out by someone else on behalf of the controller, the

the data controller may only use data processors who have appropriate guarantees

ensure that the processing complies with the requirements of this Regulation and the rights of data subjects

to implement appropriate technical and organizational measures to ensure the protection of

According to the statement of the Data Controller, the personal data collected by him / her is tabulated after processing

(.csv) format in Mailchimp and also in tabular (.csv) format

they are backed up on Sync.com. He also submitted that the databases only have it

experts with a data-processing contract who are essential for the use or maintenance of the data,

or a limited number of employees with multi-factor authentication, but access is currently not available

logged. The personal information provided by those involved is encrypted through secure channels

protected by the SSL web protocol for data transmission to the Data Controller and transmitted to the

newsletter and cloud providers.

The Privacy Statement accompanying the signature collection form did not mention data processors

only in the Data Management Information available at https://europaiugyeszseget.hu

the companies used by the Data Controller as data processors are listed.

According to the prospectus, in addition to the data processors listed separately, the Data Controller shall provide the data of

the data subjects

may be accessed by its members and staff, but a written document to that effect

provided for the tasks, activities, responsibilities to be performed by the activists, did not provide

enter the Data Manager.

9

By providing the Data Management web hosting service, DotRoll Kft. (Registered office: 1148 Budapest,

Fogarasi út 3-5.), Which according to the Data Management Information available on the website a

use an additional data processor to perform administrator and system development tasks

MICROWARE HUNGARY Kft. (registered office: 1148 Budapest, Fogarasi út 3-5.). The Data Controller a

Undated Data Processors concluded with DotRoll Kft

A copy of the agreement. According to the agreement, the task of DotRoll Kft. Is the Data Controller

the provision of the technical infrastructure, website storage, display, email service and their weekly backup for data

management.

By providing Internet marketing services, The Rocket Science Group LLC (the “

Mailchimp) and attached the Mailchimp to its reply to the Authority.

a copy of the non-signed data management appendix forming part of this Agreement.

According to the provisions of the Mailchimp e-mail service provider, automation and sales platform,

and other related services.

According to the Data Management Information, the Data Controller also uses a

Sync.com Inc. ("Sync.com"). Attached by the Data Controller between the two -

Sync.com dated June 27, 2019 - A copy of the GDPR Data Management Appendix

Inc.'s processing of personal information and other information generated solely upon the establishment of an account

contact information and personal and encrypted information provided during the service

itself. When transferring personal data and other data transferred by the Data Controller is SSL / TLS

encrypted using. Sync.com Inc. does not handle file data, file metadata,

encryption keys or passwords unless instructed to do so by the Data Controller. The Data Controller is encrypted

your data always uses end-to-end encryption and is stored with Sync.com Inc.

do not access them in a readable format or share them with third parties.

The Authority reviewed the website https://europaiugyeszseget.hu/ and found that the scanned and

signed signature collection forms could be uploaded through the interface available on the website. THE

website has SSL certification, ie the data was sent through an encrypted channel to

For data controller. Mailchimp provides 2-factor authentication based on the descriptions on the official website a

users and uses several other security procedures (eg protection against brute force). THE

Sync.com also uses 2-factor authentication according to its official website as well

protects the data of users using the cloud service with endpoint encryption.

Regarding the data processors registered abroad used by the Data Controller a

Authority found that provided by these foreign companies (Mailchimp, Sync.com)

services - the various security / encryption procedures on their website

based on a detailed description - no data security vulnerability.

However, the Authority notes that it is provided by companies established in a third country

services (including the collection, storage, organization,

and use), in particular for political opinion

in connection with the processing of personal data - poses a higher data protection risk, therefore the

It is considered good practice by the Authority if the data processing is primarily similar

EU companies providing services, thereby reducing data protection

risks.

Article 5 (2) of the GDPR provides for the principle of accountability, according to which

The data controller is responsible for ensuring that personal data is processed in accordance with the data management

principles

happen and you can prove it. An essential requirement is to allow limited access

in the case of records, to verify that only personal data are subject to authorization

authorized person, only in connection with the relevant administration.

By not logging access to the databases, the Data Controller violated

Article 5 (2) of the GDPR, as it cannot adequately prove that

whether and when the data was actually accessed, whether unauthorized access occurred.

10

In the course of his data processing, he also infringed Article 13 of the GDPR, as he did

about the data processors used during the signature collection in the Privacy Statement of the sheets

did not provide information.

With regard to the collection of signatures by activists, the Authority also draws attention to the

that the data controller has issued the signature collection form for the purpose of collecting signatures

in the case of a contract, it shall be deemed to be a data processor acting on the instructions of the controller. If it is

the data processor shall act differently from the instructions of the data controller and shall determine the purposes of the data

processing itself

and its assets shall be deemed to be a controller for the purposes of this data processing under the GDPR,

is responsible for data processing operations in this capacity.

(C) In view of the above, the Authority is required to comply with Article 58 (2) (g) of the GDPR and the Infotv.

Pursuant to Section 56 (1) 3

calls for

the Data Controller to immediately delete the "Join the European Public Prosecutor's Office!"

between 19 July 2018 and 30 May 2019 in the context of the

all personal data collected from data subjects, as their collection is valid without a legal basis

happened.

The Authority informs that Infotv. Pursuant to Section 56 (2) 4 to the Data Controller

it shall immediately take the necessary measures and shall comply with the request

within thirty (30) days of receipt of the request

Authority. The Authority will ask you to attach the cancellation documents to your reply.

Infotv. Pursuant to Section 58 (1), if, on the basis of the summons, to remedy the violation of the law, or a

the imminent threat of an infringement has not been eliminated, the Authority shall set a time limit for notification

decide on the necessary additional measures within thirty days of the expiry of the

Budapest, October 11, 2019

Best regards:

Dr. Attila Péterfalvi

President

c. professor

Infotv. § 56. (1) “If the Authority, by processing personal data or accessing data of public interest or public data in the public interest,

the existence of an infringement or imminent threat of an infringement relating to the exercise of

calls for remedial action and the elimination of its imminent danger. ".

4 Infotv. § 56. (2) “In the event of his or her consent, the data controller shall immediately take the necessary steps indicated in the notice pursuant to paragraph (1).

within 30 days of receipt of the request.

inform the Authority in writing. "