Díjnet Zrt.

PRIVACY POLICY

25 May 2018

Table of content

1. INTRODUCTION

Díjnet Zrt. as a data controller is obliged to act according to the content of this legal notice. The company assumes responsibility for ensuring that all data management related to its activity is in compliance with the regulations set out in this policy and in the applicable legislation. Information and contact details of Díjnet Zrt. are provided in Chapter 4.

Data privacy policies related to the data processing of Díjnet Zrt. are available at all times at www.dijnet.hu. Contact details of the Data Protection Officer: gdpr@dbrt.hu

Díjnet Zrt. reserves the right to change the information hereto at any time. The company will notify the users of any such changes in a timely manner.

If the user has any question that may not be clearly answered herein, please contact us, so that we can answer your question.

Díjnet Zrt. is dedicated to the data privacy of its clients and partners and believes that the clients' right for self-determination regarding their data is a matter of priority. Díjnet Zrt. treats personal information in a confidential manner and takes all security, technical and organizational measures to guarantee the security of the data.

Díjnet Zrt. hereby describes the principles of its data management and the expectations which it has self-determined of itself as data controller and which it complies with. The company's data management principles are in line with the relevant data protection laws and regulations, in particular:

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation "GDPR")

- Act CXII of 2011 on the right to informational self-determination and freedom of information ("Information Act");

- Act V of 2013 on the Civil Code ("Civil Code");

- Act C of 2000 on Accounting ("Accounting Act");

- Act CVIII of 2001 on electronic commerce services and some questions regarding the services of the informational society ("E-comm. Act");

- Act XLVIII of 2008 on the fundamental terms and some limitations of commercial advertising ("Comm. Adv. Act").

2. DATA MANAGEMENT

Díjnet Zrt performs the data management related to its activities based on the legal bases specified below for each data processing activity.

As a data provider to Díjnet Zrt., please be informed that in case you wish to provide a third party's personal data, you as a data provider are obliged to obtain the consent of the given person.

Díjnet Zrt. does not transmit data to a third country, does not use automated decision-making and reserves the right to profiling.

2.1. DATA OF THE VISITORS TO WWW.DIJNET.HU

Scope of users: visitors to www.dijnet.hu.

The purpose of the data management: during their visiting to the website, the data controller records the visitors' data to monitor the operation of the service, to provide personalized service and to prevent abuse.

The legal basis for data management: the legitimate interest of the data controller; for balance of interest, see section 7 hereto.

Scope of data to be processed: date, time, IP address, address of the page you visited, the address of the page you previously visited, and other data generally accepted for the measurement of usage during the use of the internet.

The data generated during the analysis of the log files is not combined by Díjnet Zrt. with other information, and the company does not seek to identify the user.

The duration of data management: at the end of each calendar year, the files older than 6 months are deleted from the logs of the site visits.

Data management of external service providers:

The html code of the portal contains links to external servers that are independent of Díjnet Zrt and are sourced from external servers. The server of the external service provider is connected directly to the user's computer. Please note that the providers of these links are able to collect user data by direct connection from their server and by direct communication with the user's browser.

The possibly personalized content is provided to the user by the server of the external service provider. The connection between Díjnet and the external service provider only covers the implementation of the latter's code, so no personal data is disclosed or transferred.

Advertisements may be displayed by external service providers, of which the users are informed.

2.2. COOKIE MANAGEMENT OF WWW.DIJNET.HU WEBSITE

Cookie management in the Díjnet system: Díjnet places and reads back a small data package (cookie) on user's computer in order to provide personalized service. If your browser returns a previously saved cookie, the cookie operator is able to link the user's current visit with the previous visit, but only regarding their own content. For more information about cookies and web beacons, please visit: http://www.adatvedelmiszakerto.hu/cookie.

Cookies can be deleted by the user from his computer or disabled in his browser. Generally, Cookies can be managed under the Privacy settings in the Tools/Preferences menu of the browser, usually under a label of "cookie". If you disable the cookies during the use of our website, it may result in certain features of Díjnet being inaccessible for the user.

Scope of users: visitors to www.dijnet.hu and users of the Díjnet system.

The purpose of the data management: to identify and distinguish the users, identify the user's current session, storage of data entered during the session, and prevention of data loss.

The legal basis for data management: the consent of the given user, granted or rejected by the relevant settings of the internet browser.

Scope of data to be processed: identification number, date and time.

Díjnet Zrt. uses cookies directly during the provision of the service for the following purposes:

- management of a given user session;
- store a selected language;
- switch to accessible view;
- logging the duration of time spent on the client's side.

The independent measurement and auditing of visit and other webanalytical data of www.dijnet.hu may be assisted by the server of Google Analytics and PIWIK, as external service provider. When visiting www.dijnet.hu, Google Analytics and PIWIK may process cookies in order to operate the web analytical system. For detailed information, please see the privacy policy of Google and PIWIK, available at https://www.google.com/intl/en/policies/privacy/ and http://piwik.org/privacy-policy/.

In order to track users and display personalized recommendations, Facebook can also manage cookies when using www.dijnet.hu. With remarketing, Facebook, as a partner of service, may reach the visitors of www.dijnet.hu with personalized ads on other websites which are independent of Díjnet Zrt. For the privacy policy of Facebook, please see https://www.facebook.com/about/privacy.

In addition to the above mentioned, Díjnet Zrt. also uses the Gemius RTB measurement code at www.dijnet.hu. For the cookie policy and privacy policy of Gemius please see:

- http://www.gemius.hu/cookie-szabalyok.html
- http://www.gemius.hu/az-adatkezelesrol-kiadok-szamara-akik-a-mi-kutatasunkat-hasznaljak.html

As a subcontractor of Gemius, DataXu is also involved in the measurements. For the privacy policy of DataXu, please see:

- https://www.dataxu.com/about-us/privacy/data-collection-platform/

The respective marketing partner of Díjnet Zrt. can also participate in the management of cookies associated with Facebook and Gemius services.

In addition to the above mentioned, additional cookies used by third party developers' program elements (such as javascript libraries) may be created, when using www.dijnet.hu.

The duration of the data management: two years, or the end of the session for cookies preventing data loss.

2.3. SIGN UP PROCESS FOR DÍJNET SYSTEM

Scope of users: users registered in the Díjnet system.

The purpose of the data management: to identify and distinguish the users, contact, electronic bill presentation and settlement of invoices.

The legal basis for data management: the voluntary consent of the given user, and the fulfillment of the legal obligation of the data controller in relation with a database connected to direct marketing (Article 6 (5) of Comm. Adv. Act).

Scope of data to be processed: identification number, login name, password, e-mail address, name, home address, telephone number, date of registration, time of registration, IP address of the user's computer at the time of registration, SMART card number.

Duration of data management:

- one month for non-activated Díjnet registrations,
- for user-initiated cancellations of Díjnet registration, a maximum of one month from the date that Díjnet Zrt evaluates the request.

Prohibition of direct marketing messages and deletion or modification of personal information shall be requested by the following means:

- by post mail to the address of 1518 Budapest, Postafiók 35,
- by e-mail at info@dijnet.hu - in this case please indicate in the subject field that the subject of the email is to prohibit the transfer of direct marketing messages.

2.4. REGISTRATION FOR INVOICE ISSUERS, ELECTRONIC SERVICE OF INVOICE PRESENTATION AND INVOICE PAYMENT

Data management in the registration database of invoice issuers is in connection with the Díjnet registration database, as described in Section 2.3 hereto.

Scope of users: users registered in the Díjnet system and for the invoice issuers through the system.

The purpose of the data management: to identify and distinguish the users, contact, electronic bill presentation, the logging of invoice checks done by the users, settlement of invoices and support for the users in the fulfilment of their accounting obligations.

The legal basis for data management: the voluntary consent of the given user.

Scope of data to be processed: identification number; name of the bill payer; identification data defined by the invoice issuer; date and number of one invoice issued by the given invoice issuer; date; time; data to be included in the consumer invoice; date and time of invoice checks done by the user; acceptance of direct marketing; data provided during the registration for the invoice issuer; and personal information for the transfer of which the user has given explicit consent during registration for the invoice issuer; transaction number for online payment; transaction date; transaction time; transaction amount; display name of credit card; unique identifier of credit card; a unique registration number in case of payment with online banking.

In case of online (VPOS) payment service available in Díjnet system and provided by a third party financial services provider (credit card service provided by third party), Díjnet Zrt does not constitute data controller. Díjnet Zrt. does not manage any data provided during the payment (such as credit card number, the 3-letter CVV/CVC number and card expiration date). Credit

card information may only be stored by the third-party payment service provider for the facilitation of future transactions, upon request made by the client. In connection with the aforementioned, Díjnet Zrt. only manages the display name and unique identifier of the credit card in order to make it possible for the payment service provider to choose the card that the Client would like to use for the transaction from the cards stored by him.

However, Díjnet Zrt. can provide users an online (VPOS) payment option integrated into the Díjnet system, in which case it is considered as a data controller. For this payment option, Díjbeszedő Informatikai Kft. is involved as subcontractor (data processor) of Díjnet Zrt. for fully providing the IT background of this form of payment (development, operation, maintenance) and all data management operations (eg. recording, temporary storage, modification, deletion, transmission to the payment service provider) are carried out by this company. Scope of data to be processed: credit card number, the 3-letter CVV/CVC number and card expiration date. Díjnet Zrt. does not have access to this data, the data is solely used for the performance of the given payment transaction and is deleted by Díjbeszedő Informatikai Kft. as soon as their management is no longer necessary for the given goal.

Díjnet Zrt. provides mobile payment via iCsekk service for its clients with a separate online agreement and registration, which is governed by the data protection regulations set out in iCsekk GTC and the iCsekk Privacy Statement.

Duration of data management:

Making it accessible for the user: for at least 18 months from the date of the invoice, but no longer than the date indicated in Díjnet's GTC, or until the invoice is deleted.

Storage in the Díjnet system: maximum of one month from the date of the user request for the cancellation of the registration in Díjnet system or, if this is not the case, then 5 years for accounting records and data required for the fulfillment of taxing liabilities and for the payment data of the invoices, and for other data, until the cancellation of the Díjnet registration.

The actual duration of the data processing may be less than the time limits specified here, provided that Díjnet Zrt. deletes the data, based on its own decision, within the limits provided by the Díjnet GTC.

Data forwarding:

- All the data entered during the registration will be forwarded to the selected invoice issuer for the electronic presentation of the invoices;

- When choosing a credit card payment method provided by a third party, the following is forwarded to the respective provider (payment service provider): the payer's identifier, the date, time and amount of the transaction, the name displayed on the bank card, the unique identifier of the bank card;

- In the case of an internet bank payment, the user's registration ID, the invoice expiration date, the invoice issuer's name and amount on the invoice will be forwarded to the payment service provider;

- In the case of an online (VPOS) payment option integrated into the Díjnet system, the following is forwarded to the respective provider (payment service provider): the payer's ID, the date, time and amount of the transaction, and Díjbeszedő Informatikai Kft. acting as the subcontractor of Díjnet Zrt. - without the participation of Díjnet Zrt. - forwards the bank card number, the card's three-digit identification number (CVV/CVC), and its expiration date.

- The user consumption data generated by certain invoice issuers - required for providing services according to sections 2.4. and 2.5. of this Information leaflet - are forwarded to Díjnet Zrt. by the invoice issuers in accordance with the rules laid down in the special agreement between them. The invoice issuer is responsible for the legality of this data transfer.

The legal basis for the transfer of data: the consent of the party concerned.

When paying the invoices, Díjnet Zrt. does not handle any additional personal data related to the payment.

The list of contributing card acceptors and payment service providers is published on the website by Díjnet.

*Registration with the contribution of the invoice issue*r: according to the Díjnet GTC, under certain terms, the invoice issuer registration (pre-registration and immediate registration) is performed with the contribution of the invoice issuer, or by registering through the invoice issuer in the Díjnet system. The resulting differences in data management are as follows:

- The data required for registration into the Díjnet system and for the invoice issuer registration is recorded by the invoice issuer by telephone or in person, then stored and forwarded to Díjnet Zrt. During data recording, a voice recording may take place. Throughout all of this, the invoice issuer is considered to be an independent data controller, and the detailed rules are contained in the GTC (Business Rules), Privacy Statement, Data Protection and Privacy Policy of the invoice issuer. Data processing and responsibility of Díjnet Zrt. starts with receiving the transmitted data.
- Based on the data received this way, Díjnet Zrt. will send a confirmation email to the user. Registration into the Díjnet system will be final if the user accepts the GTC, based on this e-mail. In the case of a so-called immediate invoice issuer registration, the invoice issuer registration becomes immediately active, i.e. from then, the invoice issuer presents the invoices to the client through the Díjnet system. In the case of a so-called pre-registration, the confirmation of Customer and the subsequent approval of the invoice issuer are both required for this. Starting from the finalization of the registration, in each case, general data management according to sections 2.3-2.4 of this information leaflet will be implemented.
- If the user initiated the registration to the Díjnet system through the invoice issuer, but does not approve it, Díjnet Zrt. will delete all personal data processed in connection with registration to the Díjnet system and any related data handled in relation to a possible pre-registration, initiated at the same time after the receipt of the data from the invoice issuer, within a month.
- If, in the case of pre-registration, the user does not approve the pre-registration of the invoice issuer, Díjnet Zrt. will delete all personal data related to the pre-registration, within one month of receiving the data from the invoice issuer.

2.5. INVOICE KEEPING SERVICES

Scope of interest: users registered in the Díjnet system and through the invoice issuers who have signed a Díjnet Zrt. contract for a separate invoice keeping service under the Díjnet GTC.

Purpose of data management: fulfillment of a contract for the provision of an invoice keeping service between Díjnet Zrt. and the user.

Legal basis for data processing: the fulfillment of a contract for the provision of an invoice keeping service between Díjnet Zrt and the user.

Range of data processed: is the same as listed in section 2.4.

Term of data management: service period under the contract for the provision of an invoice keeping service. If this period ends in the absence of an extension of the contract, the processing of the personal data concerned shall be governed by section 2.4. of this information leaflet.

2.6. CUSTOMER CORRESPONDENCE FOR DÍJNET ZRT.

If you have any questions or concerns about using your services, please contact Díjnet Zrt. at the contact details provided in this information leaflet.

Díjnet Zrt. assigns a tracking number to letters and customer requests received by post, and retains them along with the name of the sender and the date of arrival in its system for 5 years.

Díjnet Zrt. will delete all received e-mails, along with the sender's name and e-mail address and other voluntarily entered personal data, from the central mail system database within a maximum of 5 years from the date of disclosure.

Díjnet Zrt. will transfer those customer requests requiring reply that, based on their contents, belong to the scope of invoice issuer to the relevant invoice issuer without any change, accompanied by, if necessary, the customer ID provided at registration.

2.7. OTHER DATA MANAGEMENT PRACTICES

Information about data management practices not listed in this information leaflet is provided when data is received. Díjnet Zrt. reserves the right to send third party advertising requests electronically to customer's registered electronic contact, on the basis of a separate agreement of the client.

We inform our clients that, for the purpose of providing information, transmitting information or submitting documents, other bodies may, by virtue of the authority of the court, the public prosecutor, the investigating authority, the offense authority, the administrative authority, the National Data Protection and Information Authority may contact the Data Controller.

If the authority indicates the exact purpose of the request and scope of the data, Díjnet Zrt. issues personal data to the authorities only to the extent crucial for the purpose of the request.

3. THE WAY PERSONAL DATA IS STORED, THE SECURITY OF DATA MANAGEMENT

Computing systems and other data retention sites of Díjnet Zrt. are located at the headquarters, branches, subcontractors of the Díjbeszedő Informatikai Kft. (Headquarters: 3/a Hauszmann Alajos street, 1117 Budapest) and at the headquarters or locations of the respective Internet service provider or subcontractor. The name and contact details of the respective ISP will be published on the Website by Díjnet.

Díjnet Zrt. selects and manages the IT tools used to process personal data in the provision of the service so that the data processed:

a) is available to those entitled to it (availability);

b) has its credibility and authentication assured (credibility of data processing);

c) has verifiable integrity (data integrity);

d) is protected against unauthorized access

(confidentiality of data)

Díjnet Zrt. protects the data using appropriate measures, in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as unavailability due to accidental destruction, damage, and changing of the hardware used.

Díjnet Zrt. utilizes the right technical means to protect the data files that are electronically managed in its various registers, so that the stored data can not be directly linked and assigned to the data subject unless permitted by law.

Díjnet Zrt. provides technical, scheduling and organizational measures to protect the security of data management, in keeping with the current level of technology at all times, providing a level of protection that meets the risks associated with data management.

Throughout the data handling procedure, Díjnet Zrt. retains

a) secrecy: it protects the information, so that it can only be accessed by the person who is entitled to do so;

b) integrity: it protects the accuracy and completeness of the information and processing method;

c) availability: it ensures that when the eligible user requests it, the requested information can actually be accessed, with the related tools being available.

The IT system and network of Díjnet Zrt. and its partners are both protected against computer-aided fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer intrusions, and denial-of-service attacks. The operator provides security through server-level and application-level security procedures.

We inform the users that electronic mail, regardless of protocol (email, web, ftp, etc.) transmitted over the Internet are vulnerable to network threats that may lead to dishonest activity, contract dispute, or disclosure or modification of information. To protect it from such threats, the data controller will take all the reasonable precautionary measures. Its systems are monitored in order to record all security hazards and provide evidence of any security-related events. System monitoring also allows for checking the effectiveness of the precautions taken.

4. INFORMATION AND CONTACT DETAILS OF THE DATA CONTROLLER

Name: Díjnet Zrt.

Registered office: 107-109 Budafoki street, 1117 Budapest

Postal address: 1518 Budapest, P.O.B. 35.

Company registration number: 01-10-045817

Name of the Registry Court: Court of Registration of the Municipal Court of Budapest

Tax number: 14113765-2-43

E-mail: info@dijnet.hu

Contact details of the Data Protection Officer: gdpr@dbrt.hu

5. DATA AND CONTACT DETAILS OF DATA PROCESSORS

Díjnet Zrt. reserves the right to use a data processor, whose personal information shall be provided in a unique manner no later than at the commencement of data processing.

6. RIGHTS OF DATA SUBJECTS

Under Article 15 of the GDPR, a data subject may request access to personal data as follows:
The data subject is entitled to receive feedback from the Data Controller as to whether his or her personal data is being processed and, if such processing is in progress, has the right to have access to personal data and the following information (otherwise provided in the Privacy Policy):

a) the purposes of data management;
b) the categories of personal data concerned;
c) the categories of recipients or recipients with whom or which personal data will be communicated or disclosed, including in particular third-country addressees or international organizations;
d) where appropriate, the intended duration of the storage of personal data or, where this is not possible, the criteria for determining that period;
e) the right of the data subject to request rectification, deletion or limitation of management of his or her personal data from the data controller, and to protest against the processing of such personal data;
f) the right to lodge a complaint addressed to a supervisory authority;
g) if the data was not collected from the data subject, all available information about their source;
h) the fact of automated decision-making, including profiling, and at least in such cases, the understandable information about the logic used and the significance of such data handling and its likely consequences for the data subject.

The Data Controller shall provide the data subject with a copy of the personal data subject to data processing. For additional copies requested by the data subject, the Data Controller may charge a reasonable fee based on administrative costs. If the request has been submitted electronically, the information should be provided in a widely used electronic format, unless otherwise requested by the data subject. The right to request a copy should not adversely affect the rights and freedoms of others.

Under Article 16 of the GDPR, the data subject is entitled to request the rectification of personal data.
In case of a related request from the data subject, the Data Controller shall correct any inaccurate personal data concerning the data subject, without any undue delay. Taking into account the purpose of data management, the data subject has the right to request the amendment of incomplete personal data, including by means of a supplementary statement.

Under Article 17 of the GDPR, the person concerned has the right to request deletion of personal data, but please be aware of the following before requesting this:
The data subject has the right to request the Data Controller to delete personal data concerning him or her. In the following cases, the Data Controller shall be obliged to delete personal data concerning the data subject without any undue delay:

a) personal data is no longer needed for the purpose for which they have been collected or otherwise managed;
b) the data subject withdraws his or her consent for data processing, and there is no other legal basis for data processing;
c) the data subject objects to data processing arising from public interest, exercising of public authority rights or the legitimate interest of the data controller (third party)

and there is no high-priority legal reason for data processing or the data subject objects to data processing for direct client acquisition;

d) the personal data was illicitly handed;
e) the personal data should be deleted in order to comply with the legal obligation applicable to the Data Handler in the Union law or in the law of the Member States (Hungarian law);
f) the collection of personal data took place in connection with offering of information society services.

Right of Cancellation of the data subject can only be limited, when the following exceptions described in the GDPR exist: i.e. if the above reasons exist, further retention of personal data may be considered legitimate in the following cases, if it is necessary for:

a) the exercise of the right to freedom of expression and access to information, or
b) compliance with a legal obligation, or
c) carrying out a task in the public interest, or
d) the exercise of public authority rights conferred on the Data Controller, or
e) the public interest in the field of public health,
f) archiving arising from public interest, or
g) scientific and historical research purposes or for statistical purposes, or
h) if it is necessary to present, enforce or protect legal claims.

Under Article 18 of the GDPR, the data subject is entitled to request the Data Controller the limitation of processing of his / her personal data (as a provisional measure) as follows:
The data subject shall have the right to request that the Data Controller restricts the processing of data on request, if one of the following conditions is met:

a) the data subject disputes the accuracy of the personal data; in this case, the restriction concerns the period of time, during which the Data Controller is able to verify the accuracy of the personal data;
b) data processing is deemed illicit and the data subject is opposed to the deletion of the data, and instead requests to limit their use;
c) the Data Processor no longer needs the personal data for data processing, but the data subject requires them to submit, enforce or protect legal claims; or
d) the data subject objected to data processing due to public interest, exercise of public authority rights or legitimate interest of Data Controller (third party); in this case, the restriction is valid for that period, until it is determined that the legitimate reasons of the Data Controller have priority against the legitimate reasons of the data subject.

If the processing of data is restricted on the basis of the above, such personal data may only be processed with the consent of the data subject, or for the presentation, enforcement or protection of legal rights, or for the protection of the rights of another natural or legal person, or for complying with significant public interest of the Union or a Member State.
The Data Controller informs the data subject at whose request it has restricted the processing of data pursuant to paragraph 1, prior to the discontinuation of the restriction of data processing.

Under Article 21 of the GDPR, the data subject is entitled to object to the processing of his or her personal data by the data controller as follows:
The data subject is entitled to object to the processing of his or her personal data for public interest, for exercising public authority rights or legitimate interest of the Data Controller (third party), including profiling based on this data processing. In this case, the Data Controller may not process the personal data unless the Data Controller proves that data processing is justified

by legitimate reasons of enforceability that prevail over the interests, rights and freedoms of the data subject, or which are neccessary for the submission, enforcement or protection of legal claims.
If the personal data is processed for direct client acquisition, the data subject is entitled to object at any time to the processing of personal data for that purpose, including profiling, if it is related to direct client acquisition. If the data subject has objected to the processing of personal data for direct client acquisition, personal data may no longer be processed for that purpose.
The right to object must be explicitly referred to in the first contact with the data subject at the latest, and information about it must be clearly displayed, separated from all other kinds of information.
With respect to the use of information society services and by derogation from Directive 2002/58/EC, the data subject may also exercise his or her right to protest by automated means based on technical specifications.
If the personal data are processed for scientific and historical research purposes or for statistical purposes, the data subject is entitled to object to the processing of personal data for reasons related to his or her own personal situation, unless data processing is necessary for the execution of a task due to public interest purposes.

Under Article 20 of the GDPR, the data subject is entitled to carry personal data relating to him or her as follows:
The data subject shall have the right to receive personal data made available to him or her by a data controller in a tabbed, widely used machine-readable format and shall be entitled to transmit such data to another data controller without this being obstructed by the data controller, to whom the personal information was provided, if:

a) the legal basis for data processing is the consent of the data subject or the fulfillment of the Contract made with the data subject
b) and data processing is performed in an automated way.

In exercising the right to carry the data, the data subject is entitled to request the direct transfer of personal data between data controllers, if that is technically feasible.
The exercise of the right to carry the data shall not interfere with the right to deletion. The right to data carrying shall not apply in the case where data processing is either of public interest, or is necessary to perform a task in view of the public authority rights conferred to the Data Controller. The right to carry the data shall not adversely affect the rights and freedoms of others.

The data subject's right to appeal at a judicial authority, complaint lodged to a supervisory authority

The data subject may file a civil lawsuit against the Data Controller in case of any perceived illicit data processing. The proceedings are governed by the jurisdiction of the court. Depending on the choice of the data subject, the proceedings may be initiated at the court of the place of his or her residence (see the list of courts and their availability via the link below: http://birosag.hu/torvenyszekek
Without harm to other administrative or judicial remedies, all persons are entitled to lodge a complaint with a supervisory authority, in particular in the Member State of habitual residence, place of work or suspected infringement, if the data subject thinks that the processing of personal data relating to him or her have been infringed the GDPR.

National Data Protection and Information Authority (NAIH)

address:	22/c Szilágyi Erzsébet alley, 1125 Budapest
postal address:	1530 Budapest, P.O.B. 5
e-mail:	ugyfelszolgalat@naih.hu
phone:	+36 (1) 391-1400
fax:	+36 (1) 391-1410
website:	www.naih.hu

7. INTEREST ANALYSIS REGARDING DATA PROCESSING DESCRIBED IN SECTION 2.1

7.1. LEGAL BASIS, PROCESSED PERSONAL DATA AND PURPOSE OF DATA PROCESSING

Under Article 6 (1) (f) of the General Data Protection Regulation (2016/679/EU), "the processing of personal data is lawful only and in so far, if at least one of the following is met: [...] processing of data is necessary for enforcing the legitimate interests of the Data Controller or a third party, with the exception, that the data subjects has such interests or basic rights and freedoms that prevail over these interests, and which require the protection of personal data, particularly, if the data subject is a child".

Díjnet Zrt., as a webpage operator, in order to maintain network and IT security, processes the following personal information:

- date
- time
- IP address
- the title of the page you are visiting
- the title of the page that you visited earlier
- other data used to measure traffic data, generally accepted during internet use.

7.2. LEGITIMATE INTEREST OF THE DATA CONTROLLER

The company has a legitimate interest in the security of the IT systems of Díjnet Zrt, which is also an essential element to ensure compliance with data protection requirements. The legitimate interest in such data processing is also recognized by the General Data Protection Act itself. Under recital 49 of the Regulation, "the legitimate interests of the data controller concerned is the processing of personal data performed by public authorities, computer emergency response units (CERTs), network security incident management units (CSIRTs), providers of electronic communications networks and services and security providers, to the extent that is absolutely necessary and proportionate to guarantee network and IT security, i.e. ensuring the resilience of the network or information systems on a specific confidentiality level against random events, illicit or malicious activities, which are harmful to the data stored or transmitted on such networks and information systems, or to the accessibility, authenticity, integrity and confidental nature of such network and systems. This could include, for example, preventing unauthorized access to electronic communications networks and distribution of malware, and stopping denial of service attacks and any activities, which are harmful to computer and electronic communications systems."

7.3. DATA SUBJECT'S RIGHTS AND FREEDOMS RELATED TO PERSONAL DATA PROTECTION

The data specified above in some cases (such as a visit with a dynamic IP address) could only be linked to a specific natural person by a combination of activities from multiple data controllers. Díjnet Zrt. is unable to identify the data subject from the personal data above: the purpose of data processing is to implement certain security measures related to IT systems based on logged data or, where appropriate, to initiate a specific legal process in case a visitor to the website is liable for any illicit activity related to the visit to the website. Otherwise, the data will not be used by the Data Controller or any third party to identify a visitor to the website. In a general case, the processing of data does not affect the privacy of the data subject, and the processing of the data in question does not pose a threat to the rights and freedoms of the data subject.

7.4. RESULTS OF INTEREST ANALYSIS

In the interest analysis, it was found that (1) the controller is legitimate, supported by the text of GDPR and has explicit interest of the security of its IT system as a result of the data protection provisions; and (2) the privacy of the data subject is not affected by data processing (provided that the data subject does not commit an illicit act), for in a general case, neither the data controller, nor a third party uses data processed for identification of the data subject. Since data processing is necessary for enforcing the legitimate interests of the Data Controller and the interests or fundamental rights and freedoms of the data subject that require the protection of personal data do not prevail over these interests, the data specified above are to be processed by Díjnet Zrt., in accordance with Article 6 (1) (f) of the General Data Protection Regulation.