Díjnet Zrt.

PRIVACY POLICY

04 November 2020

Table of contents

1. INTRODUCTION

Díjnet Zrt. as a data controller and data processor 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 legjslation. Information and contact details of Díjnet Zrt. are provided in Chapter 4. For the purposes of data management when Díjnet Zrt. handles data in another name, Díjnet Zrt. is data processor. In such cases, the privacy policy of the data controller is normative and Díjnet Zrt. shall set out its data processing obligations in this document.

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@dijnet.hu

In the case of certain services and promotions, Díjnet Zrt. may issue individual data management information at the time of using the service or in the case of promotion at the first contact.

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 ofitself 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 CVHI 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").

- In addition to the above, other laws and other legal guidelines may also be relevant, which Díjnet Zrt. provides in individual cases.

2. DATA MANAGEMENT

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 fles 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 fles 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.

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, as external service provider. When visiting www.dijnet.hu, Google Analytics may process cookies in order to operate the web analytical system. For detailed information, please see the privacy policy of Google, available at https://www.google.com/intl/en/policies/privacy/ .

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.

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

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 DIJNET SYSTEM

Scope of users: users registered in the Díjnet system.

The purpose of the data management: distinguish the users, creating and maintaining a registration for an invoice presentation service, accessing services; use and maintenance of bill payment and related services; sending e-mails related to the performance of the service.

The legal basis for data management: data management is necessary for the performance of the contract (Article 6 (1.b.) of GDPR).

Scope of data to be processed: identfication 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.

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.

2.4. DÍJNET NEWSLETTER

Díjnet Zrt. sends direct marketing messages in the form of electronic newsletters to users who have granted their express consent.

Registered users may provide declarations of consent to Díjnet Zrt. after logging in to their user account.

Purpose of data processing: sending e-mail newsletters including business advertisements to interested parties, personalisation of newsletters, providing current information, preparing personalised offers,

communications, forwarding business offers by the data controller and its partners.

Legal basis for data processing: the freely given consent of the data subject [GDPR Article 6 (1) a)].

Types of personal data processed: identification number, date, time, e-mail address, name, consent to direct marketing inquires, moreover, the system stores information regarding subscription, unsubscription and sending messages.

Duration of data processing:

- until withdrawal of the user's consent but no longer than
- 24 months after the user's last data update

Possible consequences of failure to provide relevant data: the data subject is not informed of the offers by the data controller and its partners.

Users may withdraw their consent to the forwarding of direct marketing messages and request erasure or amendment of their personal data by the following means:

- by logging in to the user account in the "User Details" menu item,
- by email sent to ugyfelszolgalat@dijnet.hu moreover
- by mail to Díjnet Zrt., 1117 Budapest, Budafoki út 107-109.

2.5. 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.

The legal basis for data management: the voluntary consent of the given user and the contract with the service provider as data controller.

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; 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 fnancial 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): vide section 2.5.1;

- 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 issuer: 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 fnal 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 confrmation of Customer and the subsequent approval of the invoice issuer are both required for this. Starting from the fnalization 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.

2.5.1 Strong Customer Authentication, SCA

Description, process and content of data management: The electronic payment service is to be performed in a secure manner, using technologies that guarantee the secure identification of the user of the service and minimize the risk of fraud. The authentication process includes transaction-monitoring mechanisms to detect unauthorized attempts to use lost, stolen data or personal credentials of the payment service users, as well as to ensure, that the payment service user is the legitimate user, giving consent to the payment service by using personal credentials.

Therefore, during the use of the Service, the Service Provider transmits the data, specified in this chapter, to the payment service provider supporting the Service to perform the payment transaction by identifying the customer.

The purpose of data management: To secure the payment transaction during the use of the Application by identifying the customer.

Legal basis for data management: Fulfillment of a legal obligation on the data controller (Article 6 (1.c.) of GDPR). The legal obligation is based on the article of Commission Delegated Regulation (EU) 2018/389 / supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open communication standards / Articles 1 and 24, and LXXXV of 2009. Act 55 / C.

The scope of the managed data: Name, address, e-mail address used for payment, telephone number, transaction ID, amount and currency of the transaction.

Duration of data management: Until the handover of the e-mail address used for payment to the payment service provider has been completed.

2.6. INVOCE KU PIM, 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: fufillment 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.

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. RIGHTS OF DATA SUBJECTS

If Díjnet Zrt. is the data processor, the rights of the data subject may be asserted against the relevant public utility provider.

If Díjnet Zrt. is the data controller, the data subject (or their duly authorised representative) shall have the following rights under Articles 13-21 of the GDPR.

The data subject shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information (otherwise provided in the Privacy Policy):

a) the purposes of data processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data was not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The Controller shall provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, the Controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise

requested by the data subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Under Article 16 of the GDPR, the data subject shall have the right to request the rectification of personal data.

Upon request of the data subject, the Controller shall rectify any inaccurate personal data concerning the data subject, without any undue delay. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Under Article 17 of the GDPR, the data subject shall have the right to request the erasure of personal data, but please be aware of the following before requesting this:

The data subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her. In the following cases, the Controller shall have the obligation to erase personal data concerning the data subject without any undue delay:

a) the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;

c) the data subject objects to data processing carried out in the public interest, in the exercise of official authority or in the legitimate interest of the data controller (third party) and there are no overriding legitimate grounds for the processing, or the data subject objects to data processing for direct marketing purposes;

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law (Hungarian law) to which the controller is subject;

f) the personal data have been collected in relation to the offer of information society services.

The Data Subject's right to erasure can only be restricted, when the following exceptions described in the GDPR exist: i.e. if the above reasons exist, further retention of personal data should be lawful in the following cases, where it is necessary for:

a) exercising the right of freedom of expression and access to information, or

b) compliance with a legal obligation, or

c) performance of a task carried out in the public interest, or

d) the exercise of official authority vested in the controller, or

e) on the grounds of public interest in the area of public health,

f) for archiving purposes in the public interest, or

g) scientific and historical research purposes or for statistical purposes, or

h) if it is necessary for the establishment, exercise or defence of legal claims.

Under Article 18 of the GDPR, the data subject shall have the right to request from the Controller restriction of processing of personal data concerning him or her (as a provisional measure) as follows:

The data subject shall have the right to obtain from the Controller restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the Controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

d) the data subject has objected to processing in the public interest, in the exercise of official authority or in the legitimate interest of the controller (third party); pending the verification whether the legitimate grounds of the Controller override those of the data subject.

Where processing has been restricted as per the above, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the Controller before the restriction of processing is lifted.

Under Article 21 of the GDPR, the data subject shall have the right to object to the processing of personal data concerning him or her by the Data Controller as follows:

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is performed in public interest, in the exercise of official authority or in the legitimate interest of the controller (third party), including profiling based on such data processing. In this case, the Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the right to object shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Under Article 20 of the GDPR, the data subject shall have the right to data portability in respect of the data concerning him or her as follows:

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) the legal basis for data processing is the consent of the Data Subject or the performance of a contract entered into with the Data Subject

b) and the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The exercise of the right to data portability shall be without prejudice to the right to erasure. The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The right to data portability shall not adversely affect the rights and freedoms of others.

5. 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@dijnet.hu

6. RIGHT TO LEGAL REMEDY

Right to judicial remedy:

The data subject may resort to judicial remedy against the data controller if his or her rights are infringed. The procedure may be initiated at the Budapest-Capital Regional Court or, depending on the choice of the data subject, 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

Procedures before the competent data protection authority:

Complaints may be lodged by e-mail to gdpr@dijnet.hu or regular mail to 1117 Budapest, Budafoki út 107. If Díjnet Zrt. is a data processor, it will forward the relevant complaints to the data controller within a reasonable period of time.

Where the data controller fails to fulfil the complainant's request, the case may be referred to the Hungarian National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság) or directly to the competent court:

Name: Hungarian National Authority for Data Protection and Freedom of Information (NAIH)

Registered office: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Postal address: 1530 Budapest, Pf.: 5.

Phone: 06 1 391 1400

Fax: 06 1 391 1410

E-mail: ugyfelszolgalat@naih.hu

Website: http://www.naih.hu