PRIVACY NOTICE

for the data processing activities carried out by NEBET.HU Kft. on the websites idokapuszoftver.hu, idokapu.nebet.hu, gatebooking.hu, gatebooking.sk, gatebooking.de, gatebooking.ch, gatebooking.at, gatebooking.eu and ro.gatebooking.eu

Effective from 1 May 2026

Contents

Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), we provide the following information.

This Privacy Notice regulates the data processing activities of the following websites/mobile applications:
https://idokapuszoftver.hu

The Privacy Notice is available at:
https://www.idokapuszoftver.hu/adatvedelem

Amendments to this Notice enter into force upon publication at the above address.

Name of the Controller

NEBET.HU Kft.

Item	Details
Address	Hungary, H-2890 Tata, Újhegyi út 70.
Telephone	+36 20 288 9591
E-mail	info@nebet.hu
Website	nebet.hu

Nebet.hu Kft. has not appointed a data protection officer.

Definitions

“personal data”: any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

“processing”: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“controller”: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

“processor”: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

“recipient”: a natural or legal person, public authority, agency or another body to which personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; processing of those data by those public authorities shall comply with the applicable data protection rules according to the purposes of the processing;

“consent of the data subject”: any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

“personal data breach”: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Principles relating to the processing of personal data

Personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”);
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) shall not be considered incompatible with the initial purposes (“purpose limitation”);
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods only where the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).

The Controller is responsible for compliance with the above and must be able to demonstrate such compliance (“accountability”).

The Controller declares that its processing activities are carried out in accordance with the principles set out in this section.

Categories of data processed

Data processing related to the use of the service

The fact of data collection, the categories of data processed and the purpose of processing:

In the case of a purchase with a receipt, only the e-mail address is stored. The purpose is contact management, and the legal basis is Article 6(1)(b) GDPR and Section 13/A(3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (“E-Commerce Act”).

In the case of a purchase with registration:

Personal data	Purpose of processing	Legal basis
Password	Secure access to the user account.	Article 6(1)(b) GDPR and Section 13/A(3) of the E-Commerce Act.
E-mail address	Contact management.	Article 6(1)(b) GDPR and Section 13/A(3) of the E-Commerce Act.
Billing name and address	Issuing a proper invoice, creating, defining the content of, amending and performing the contract, monitoring performance, invoicing fees arising from the contract and enforcing related claims.	Article 6(1)(c) GDPR and Section 169(2) of Act C of 2000 on Accounting.

Personal data	Purpose of processing	Legal basis
Date of registration and last login	Performance of a technical operation.	Article 6(1)(b) GDPR and Section 13/A(3) of the E-Commerce Act.
IP address at registration	Performance of a technical operation.	Article 6(1)(b) GDPR and Section 13/A(3) of the E-Commerce Act.

The e-mail address does not necessarily have to contain personal data.

Data subjects concerned: all data subjects registered on the website or using the service.

Duration of processing and deadline for erasure: where any of the conditions set out in Article 17(1) GDPR apply, processing lasts until the erasure request of the data subject. Pursuant to Article 19 GDPR, the Controller informs the data subject electronically of the erasure of any personal data provided by the data subject. If the erasure request also covers the e-mail address provided by the data subject, the Controller will erase the e-mail address after providing the information. This does not apply to accounting documents, since pursuant to Section 169(2) of Act C of 2000 on Accounting, such data must be retained for 8 years. Contractual data relating to the data subject may be erased upon the data subject's erasure request after the expiry of the civil law limitation period.

Accounting documents directly and indirectly supporting bookkeeping records, including general ledger accounts, analytical and detailed records, must be kept in a readable form for at least 8 years and in a manner retrievable by reference to the accounting records.

Possible controllers entitled to access the data and recipients of personal data: the personal data may be processed by the Controller's sales and marketing staff, in compliance with the above principles.

Description of data subject rights related to processing:

- The data subject may request from the Controller access to personal data concerning him or her, rectification or erasure of such data, or restriction of processing.
- The data subject has the right to data portability and the right to withdraw consent at any time.

The data subject may initiate access to, erasure or modification of personal data, restriction of processing and data portability in the following ways:

- by post to H-2890 Tata, Újhegyi út 70.;
- by e-mail to info@nebet.hu;
- by telephone on +36 20 288 9591.

Legal basis of processing:

- Article 6(1)(b) and (c) GDPR;
- Section 13/A(3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services ("E-Commerce Act"): the service provider may process personal data that are technically indispensable for providing the service. Other conditions being equal, the service provider must choose and operate the tools used in providing information society services in such a way that personal data are processed only where strictly necessary for providing the service and for fulfilling the other purposes specified in the Act, and even then only to the extent and for the period necessary;
- where an invoice compliant with accounting legislation is issued: Article 6(1)(c) GDPR;
- in the case of enforcing claims arising from a contract: 5 years pursuant to Section 6:21 of Act V of 2013 on the Civil Code.

Section 6:22 [Limitation]

1. Unless otherwise provided by law, claims become time-barred after five years.
2. The limitation period begins when the claim becomes due.
3. An agreement to change the limitation period must be made in writing.

4. An agreement excluding limitation is null and void.

Please note that:

- processing is necessary for performance of the contract and for providing an offer;
- you are required to provide the personal data so that we can fulfil your order;
- failure to provide the data will result in our inability to process your order.

Complaint handling

The fact of data collection, the categories of data processed and the purpose of processing:

Personal data	Purpose of processing	Legal basis
Surname and first name	Identification and contact management.	Article 6(1)(c) GDPR and Section 17/A(7) of Act CLV of 1997 on Consumer Protection.
E-mail address	Contact management.	Article 6(1)(c) GDPR and Section 17/A(7) of Act CLV of 1997 on Consumer Protection.
Telephone number	Contact management.	Article 6(1)(c) GDPR and Section 17/A(7) of Act CLV of 1997 on Consumer Protection.
Billing name and address	Identification and handling quality objections, questions and problems related to ordered products/services.	Article 6(1)(c) GDPR and Section 17/A(7) of Act CLV of 1997 on Consumer Protection.

Data subjects concerned: all data subjects purchasing on the website and making a quality complaint or lodging a complaint.

Duration of processing and deadline for erasure: copies of the minutes, transcript and response relating to the complaint must be retained for 3 years pursuant to Section 17/A(7) of Act CLV of 1997 on Consumer Protection.

Possible controllers entitled to access the data and recipients of personal data: the personal data may be processed by the Controller and its authorised employees, in compliance with the above principles.

Description of data subject rights related to processing:

- The data subject may request from the Controller access to personal data concerning him or her, rectification or erasure of such data, or restriction of processing; and
- the data subject has the right to data portability and the right to withdraw consent at any time.

The data subject may initiate access to, erasure or modification of personal data, restriction of processing and data portability by post to H-2890 Tata, Újhegyi út 70., by e-mail to info@nebet.hu, or by telephone on +36 20 288 9591.

Please note that:

- the provision of personal data is based on a legal obligation;
- processing of personal data is a precondition for concluding the contract;
- you are required to provide the personal data so that we can handle your complaint;
- failure to provide the data will result in our inability to handle the complaint received from you.

Customer relations

The fact of data collection, the categories of data processed and the purpose of processing:

Personal data	Purpose of processing	Legal basis
Name, e-mail address, telephone number.	Contact management, identification, performance of contracts and business purposes.	Article 6(1)(b) and (c) GDPR; in the case of enforcing claims arising from a contract, Section 6:21 of Act V of 2013 on the Civil Code.

Data subjects concerned: all data subjects who maintain or establish contact with the Controller by telephone, e-mail, in person or via a form, or who have a contractual relationship with the Controller.

Duration of processing and deadline for erasure: letters containing enquiries are retained until the data subject's erasure request, but for a maximum of 2 years.

Possible controllers entitled to access the data and recipients of personal data: the personal data may be processed by the Controller's authorised employees, in compliance with the above principles.

Description of data subject rights related to processing:

- The data subject may request from the Controller access to personal data concerning him or her, rectification or erasure of such data, or restriction of processing; and
- the data subject has the right to data portability and the right to withdraw consent at any time.

The data subject may initiate access to, erasure or modification of personal data, restriction of processing and data portability by post to H-2890 Tata, Újhegyi út 70., by e-mail to info@nebet.hu, or by telephone on +36 20 288 9591.

Legal basis of processing: the consent of the data subject and Article 6(1)(a) and (b) GDPR. If you contact us, you consent to the processing, in accordance with this Notice, of the personal data provided to us during the contact process (name, telephone number, e-mail address).

Please note that:

- processing is necessary for performance of the contract and for providing an offer;
- you are required to provide the personal data so that we can perform the contract or fulfil your other request;
- failure to provide the data will result in our inability to perform the contract or process your request.

Cookie management

Prior consent of data subjects is not required for the use of so-called "cookies used for password-protected sessions", "cookies necessary for the shopping cart", "security cookies", "strictly necessary cookies", "functional cookies" and "cookies responsible for managing website statistics".

Fact of processing and categories of data processed: unique identification number, dates and times.

Data subjects concerned: all visitors to the website.

Purpose of processing: identifying users, tracking visitors and ensuring customised operation.

Duration of processing and deadline for erasure:

Type of cookie	Legal basis of processing	Duration of processing
Session cookies or other cookies strictly necessary for the operation of the website	Article 6(1)(f) GDPR. The Controller's legitimate interest in operating the website, ensuring the functionality and basic functions of the website, and the security of the computer system.	Until the end of the relevant visitor session.
Persistent or stored cookies	Article 6(1)(f) GDPR. The Controller's legitimate interest in operating the website, ensuring the functionality and	Processing lasts until erasure by the data subject; cookies with a precise validity period are stored on the computer until

Type of cookie	Legal basis of processing	Duration of processing
	basic functions of the website, and the security of the computer system.	they are deleted, but no later than the expiry of their validity period.
Statistical and marketing cookies	Article 6(1)(a) GDPR.	1 month to 2 years.

Possible controllers entitled to access the data: the personal data may be accessed by the Controller.

Description of data subject rights related to processing: data subjects can delete cookies in the Tools/Settings menu of their browsers, usually under the Privacy settings.

Most browsers used by our users allow users to set which cookies should be saved and allow specified cookies to be deleted again. If you restrict the saving of cookies on certain websites or do not allow third-party cookies, this may, in certain circumstances, result in our website no longer being fully usable. Information on how to customise cookie settings in common browsers is available here:

- Google Chrome (https://support.google.com/chrome/answer/95647?hl=hu)
- Internet Explorer (https://support.microsoft.com/hu-hu/windows/cookie-k-t%C3%B6rl%C3%A9se-%C3%A9s-kezel%C3%A9se-168dab11-0753-043d-7c16-ede5947fc64d)
- Microsoft Edge (https://support.microsoft.com/hu-hu/microsoft-edge/cookie-k-t%C3%B6rl%C3%A9se-a-microsoft-edge-ben-63947406-40ac-c3b8-57b9-2a946a29ae09)
- Firefox (https://mzl.la/3vVeO8Y)
- Safari (https://support.apple.com/hu-hu/guide/safari/sfri11471/mac)

Use of Google Analytics

1. This website uses Google Analytics, a web analytics service provided by Google Inc. (“Google”). Google Analytics uses so-called “cookies”, text files saved on your computer, which help analyse the use of the website visited by the User.
2. The information generated by cookies about the website used by the User is generally transmitted to and stored on a Google server in the USA. If IP anonymisation is activated on the website, Google will shorten the User’s IP address beforehand within Member States of the European Union or in other states party to the Agreement on the European Economic Area.
3. Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and shortened there. On behalf of the operator of this website, Google will use this information to evaluate how the User used the website, to compile reports for the website operator on website activity, and to provide further services relating to website and internet usage.
4. The IP address transmitted by the User’s browser within the framework of Google Analytics will not be merged with other Google data. The User can prevent the storage of cookies by selecting the appropriate settings in the browser; however, please note that in this case not all functions of this website may be fully usable. The User can also prevent Google from collecting and processing data generated by cookies and relating to website use, including the IP address, by downloading and installing the browser plug-in available at: https://tools.google.com/dlpage/gaoptout?hl=hu

Processor activity	Name	Address, contact details
Statistical reports	Google Analytics	Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA https://policies.google.com/privacy

Facebook Pixel

The Facebook Pixel is a code that enables conversion reporting on the website, the creation of audiences, and detailed analytics for the website owner regarding visitors’ use of the website. With the help of the Facebook

Pixel, personalised offers and advertisements may be displayed to website visitors on Facebook. If you do not accept the use of cookies, certain functions will not be available to you.

Processor activity	Name	Address, contact details
Analytics and ad optimisation	Facebook	Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland https://www.facebook.com/privacy/policy/

Recipients with whom personal data are disclosed:

"recipient" means a natural or legal person, public authority, agency or another body to which personal data are disclosed, whether a third party or not.

Processors

(persons or entities that process data on behalf of the Controller)

Processors carry out processing on behalf of the Controller.

In order to facilitate its own processing activities and to fulfil its contractual and legal obligations towards data subjects, the Controller uses processors.

The Controller attaches great importance to using only processors that provide sufficient guarantees to implement appropriate technical and organisational measures ensuring compliance with the GDPR requirements and the protection of data subjects' rights.

The processor and any person acting under the authority of the Controller or the processor who has access to personal data may process the personal data set out in this Notice only in accordance with the Controller's instructions.

The Controller bears legal responsibility for the activities of the processor. The processor is liable for damage caused by processing only where it has not complied with obligations under the GDPR specifically directed to processors, or where it has acted outside or contrary to lawful instructions of the Controller.

The processor does not have substantive decision-making powers regarding the processing of data.

Processor activity	Name	Address, contact details
Hosting service	Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Germany; +49 9831 505-0; info@hetzner.com
Invoicing	KBOSS.hu Kft.	1031 Budapest, Záhony utca 7.; info@szamlazz.hu; https://www.szamlazz.hu/adatvedelem/

Data transfer

Third-party controllers process the personal data disclosed by us in their own name and in accordance with their own privacy policies.

Online payment

Activity performed by the recipient: online payment.

Fact of processing and categories of data processed: billing data, name and e-mail address.

Data subjects concerned: all data subjects selecting payment on the website.

Purpose of processing: processing online payment, confirming transactions and fraud monitoring performed to protect users.

Duration of processing and deadline for erasure: until the online payment has been processed.

Legal basis of processing: Article 6(1)(b) GDPR. Processing is necessary for performing the online payment requested by the data subject.

Rights of the data subject:

- The data subject may obtain information about the circumstances of processing.
- The data subject is entitled to receive confirmation from the Controller as to whether his or her personal data are being processed and to access all information relating to the processing.
- The data subject is entitled to receive the personal data concerning him or her in a structured, commonly used, machine-readable format.
- The data subject is entitled to request that the Controller rectify inaccurate personal data concerning him or her without undue delay.

Processor activity	Name	Address, contact details
Online bank card payment	OTP SimplePay	OTP Mobil Szolgáltató Kft., Budapest, Váci út 135-139.; ugyfelszolgalat@simple.hu; +36 1 3666 611; https://simplepay.hu/adatkezelesi-tajekoztatok/

Customer contacts and other processing activities

1. If, during the use of the Controller's services, the data subject has a question or problem, he or she may contact the Controller using the methods provided on the website (telephone, e-mail, social media pages, etc.).
2. The Controller deletes incoming e-mails, messages and data provided by telephone, on Meta, etc., together with the name and e-mail address of the enquirer and any other personal data voluntarily provided, no later than 2 years after the data disclosure.
3. Information on processing activities not listed in this Notice is provided at the time of data collection.
4. In the event of exceptional requests from authorities or requests from other bodies based on statutory authorisation, the Service Provider is obliged to provide information, disclose or transfer data, or make documents available.
5. In such cases, the Service Provider discloses personal data to the requesting party, provided that the precise purpose and scope of data have been indicated, only to the extent and in the amount indispensable for achieving the purpose of the request.

Social media pages

1. **Fact of data collection and categories of data processed:** the name registered on Meta/Twitter/Pinterest/YouTube/Instagram and other social media pages, and the user's public profile picture.
2. **Data subjects concerned:** all data subjects registered on Meta/Twitter/Pinterest/YouTube/Instagram or other social media pages who have "liked" the Service Provider's social media page or contacted the Controller via the social media page.
3. **Purpose of data collection:** sharing, "liking", following and promoting certain content elements, products, promotions or the website itself on social media pages.
4. **Duration of processing, deadline for erasure, possible controllers entitled to access the data and description of data subject rights related to processing:** the data subject may obtain information on the source of the data, their processing, the method of transfer and the legal basis on the relevant social media page. Processing takes place on the social media pages; therefore the rules of the relevant social media page apply to the duration and method of processing and to the possibilities of erasure and modification.
5. **Legal basis of processing:** the data subject's voluntary consent to the processing of his or her personal data on social media pages.

Rights of data subjects

1. Right of access

You have the right to obtain from the Controller confirmation as to whether or not personal data concerning you are being processed and, where such processing is taking place, access to the personal data and to the information listed in the Regulation.

2. Right to rectification

You have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3. Right to erasure

You have the right to obtain from the Controller the erasure of personal data concerning you without undue delay, and the Controller has the obligation to erase personal data concerning you without undue delay where certain conditions apply.

4. Right to be forgotten

Where the Controller has made the personal data public and is obliged to erase it, the Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers processing the personal data that you have requested the erasure of any links to, or copy or replication of, those personal data.

5. Right to restriction of processing

You have the right to obtain from the Controller restriction of processing where one of the following applies:

- you contest the accuracy of the personal data, for a period enabling the Controller to verify the accuracy of the personal data;
- the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- the Controller no longer needs the personal data for the purposes of processing, but you require them for the establishment, exercise or defence of legal claims;
- you have objected to processing; in this case the restriction applies pending verification whether the legitimate grounds of the Controller override your legitimate grounds.

6. Right to data portability

You have the right to receive the personal data concerning you, which you have 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 (…).

7. Right to object

In the case of processing based on legitimate interest or the exercise of public authority, you have the right to object, on grounds relating to your particular situation, at any time to the processing of personal data concerning you, including profiling based on those provisions.

8. Objection to direct marketing

Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for such marketing, including profiling to the extent that it is related

to such direct marketing. Where you object to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

9. Automated individual decision-making, including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which would produce legal effects concerning you or similarly significantly affect you.

The preceding paragraph does not apply if the decision:

- is necessary for entering into, or performance of, a contract between you and the Controller;
- is authorised by Union or Member State law to which the Controller is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or
- is based on your explicit consent.

Time limit for taking action

The Controller informs you without undue delay, and in any event within 1 month of receipt of the request, of the action taken on the above requests.

Where necessary, this period may be extended by 2 months. The Controller informs you of any such extension within 1 month of receipt of the request, together with the reasons for the delay.

If the Controller does not take action on your request, the Controller informs you without delay and at the latest within one month of receipt of the request of the reasons for not taking action and of the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Security of data processing

Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and the processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, where appropriate, among others:

1. pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services used for processing personal data;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing;
5. the processed data must be stored in such a way that unauthorised persons cannot access them. In the case of paper-based data carriers, this is ensured by establishing rules for physical storage and archiving; in the case of electronically processed data, by using a central access management system;
6. the method of storing data by IT means must be selected so that the data can be erased when the erasure deadline expires, taking into account any different erasure deadlines, or whenever otherwise necessary. Erasure must be irreversible;
7. paper-based data carriers must be stripped of personal data using a shredder or by using an external organisation specialised in document destruction. In the case of electronic data carriers, physical destruction must be ensured in accordance with the rules on disposal of electronic data carriers, and, where necessary, secure and irreversible erasure of data must be carried out beforehand;
8. the Controller applies the following specific data security measures:

Physical protection

In order to ensure the security of personal data processed on paper, the Service Provider applies the following measures:

1. Documents must be placed in a secure, well-lockable dry room.
2. If personal data processed on paper are digitised, the rules applicable to digitally stored documents must be applied.
3. During work, the employee of the Service Provider performing processing may leave the room where processing is taking place only after locking away the entrusted data carriers or locking the room.
4. Personal data may be accessed only by authorised persons; third parties may not access them.
5. The Service Provider's building and premises are equipped with fire protection and property protection equipment.

IT protection

1. The computers and mobile devices (and other data carriers) used during processing are owned by the Service Provider.
2. The computer system containing personal data used by the Service Provider is protected against viruses.
3. In order to ensure the security of digitally stored data, the Service Provider uses backups and archiving.
4. The central server may be accessed only with appropriate authorisation and only by designated persons.
5. Data stored on computers may be accessed only with a username and password.

Informing the data subject about a personal data breach

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller informs the data subject without undue delay.

The communication to the data subject must describe, in clear and plain language, the nature of the personal data breach and must communicate the name and contact details of the data protection officer or other contact point from whom more information can be obtained; it must describe the likely consequences of the personal data breach and the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The data subject does not have to be informed if any of the following conditions are met:

- the Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular measures such as encryption that render the personal data unintelligible to any person who is not authorised to access it;
- the Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
- informing the data subject would involve disproportionate effort. In such cases, data subjects must be informed by means of publicly available information or a similar measure that ensures similarly effective information of the data subjects.

If the Controller has not yet notified the data subject of the personal data breach, the supervisory authority, having considered whether the personal data breach is likely to result in a high risk, may require the Controller to do so.

Notification of a personal data breach to the authority

The Controller notifies the personal data breach to the supervisory authority competent under Article 55 without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, it must be accompanied by reasons for the delay.

Review in the case of mandatory data processing

If the duration of mandatory processing or the periodic review of its necessity is not determined by law, local government decree or a binding legal act of the European Union, the Controller reviews, at least every three years from the start of processing, whether the processing of personal data by the Controller or by a processor acting on its behalf or under its instructions is necessary for achieving the purpose of processing.

The Controller documents the circumstances and results of this review, retains this documentation for ten years after the review has been carried out, and makes it available to the National Authority for Data Protection and Freedom of Information (hereinafter: “Authority”) at the Authority’s request.

Right to lodge a complaint

A complaint concerning any infringement by the Controller may be lodged with the National Authority for Data Protection and Freedom of Information:

National Authority for Data Protection and Freedom of Information
1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf. 9.
Telephone: +36 1 391 1400
Fax: +36 1 391 1410
E-mail: ugyfelszolgalat@naih.hu

Closing provisions

In preparing this Notice, we took into account the following legislation:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing 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 (“Privacy Act”);
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services, especially Section 13/A;
- Act XLVII of 2008 on the prohibition of unfair commercial practices against consumers;
- Act XLVIII of 2008 on the basic requirements and certain restrictions of commercial advertising activities, especially Section 6;
- Act XC of 2005 on electronic freedom of information;
- Act C of 2003 on electronic communications, in particular Section 155;
- Opinion No. 16/2011 on the EASA/IAB Best Practice Recommendation on online behavioural advertising;
- The recommendation of the National Authority for Data Protection and Freedom of Information on the data protection requirements of prior information.