DATA PROCESSING NOTICE

1. INTRODUCTION

This Data Processing Notice (hereinafter: **Notice**) applies to the processing of personal data arising in the context of the operation of the www.babolnatakarmany.hu website of **Bonafarm-Bábolna Takarmány Kft.** (hereinafter the **Controller**). The Controller pays particular attention to the protection of personal data, to compliance with legal regulations and to secure and fair data processing.

Contact details of the Controller:

Name:	Bonafarm-Bábolna Takarmány Kft.
Mailing address:	H-2942 Nagyigmánd, Burgert Róbert Agrár-Ipari park 03/25 hrsz
Email address:	info@babolnatakarmany.hu
Website:	www.babolnatakarmany.hu
Telephone number:	+36-34-557-050

Contact details of the Controller's representative:

Name:	Gergely Balassa
Mailing address:	H-2942 Nagyigmánd, Burgert Róbert Agrár-Ipari park 03/25 hrsz
Email address:	info@babolnatakarmany.hu
Telephone number:	+36-34-557-050

This Notice has been drafted based on the following legal regulations in particular:

a) Act CXII of 2011 on Informational Self-Determination and the Freedom of Information (hereinafter the **Privacy Act**);
b) Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society-Related Services (hereinafter the **E-commerce Act**);
c) Act XLVIII of 2008 on the Essential Conditions of and Certain Limitations on Business Advertising (hereinafter the **Advertising Act**);
d) Act C of 2003 on Electronic Communications (hereinafter the **Electronic Communications Act**);
e) 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 (hereinafter the **Regulation**).

This Notice is available at the following site: www.bonafarmcsoport.hu/adatkezelesi-tajekoztato

The Controller reserves the right to amend this Notice, in which case such amendments enter into force by publication on the following website: www.bonafarmcsoport.hu/adatkezelesi-tajekoztato.

2. DEFINITIONS

The terms used in this Notice shall have the following meaning:

data subject: a natural person identified or identifiable based on any information (Section 3(1) of the Privacy Act); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier or to one or more factors specific to that natural person (Article 4(1) of the Regulation);

personal data*:* any information relating to the data subject (Section 3(2) of the Privacy Act) – in particular identifiers such as a name, an identification number, location data, online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags (RFID) (Recital (30) of the Regulation), or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person – as well as any conclusions drawn from such information and data pertaining to the data subject (Article 4(1) of the Regulation).

data processing: irrespective of the procedure followed, any operation or the totality of operations performed on the data, including in particular collection, admission, recording, organisation, storage, adaptation, utilisation, retrieval, consultation by transmission, disclosure, alignment or combination, restriction, blocking, erasure or destruction and the preventing further use of such data, the taking of photos, recording of audio signals or images, as well as the recording of physical properties suitable for identifying a person (including fingerprint and palmprint, DNS sample and iris image) (Article 4(2) of the Regulation; Section 3(10) of the Privacy Act);

data controller: the natural person or legal entity or organisation without legal personality who/which determines, either individually or in cooperation with others, the purpose and instruments of data processing, adopts and implements, or ensures the implementation of decisions on data processing (including the tools to be used) by data processor (Article 4(7) of the Regulation; Section 3(9) of the Privacy Act);

data processing: performance of technical tasks related to data processing operations, regardless of the methods and instruments used for executing such operations, and of the place of application, assuming that such technical task is performed on the data (Section 3(17) of the Privacy Act);

data processor: the natural or legal person or the organisation without legal personality, public authority, agency or other body who/which, under a contract concluded with the controller, including contracts concluded by virtue of a legal provision, processes personal data on behalf of the controller (Article 4(8) of the Regulation; Section 3(18) of the Privacy Act);

representative of the controller / processor: a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under the Regulation (Article 4(17) of the Regulation);

third party: a natural person or legal entity or organisation without legal personality, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, perform operations aimed at processing personal data or are authorised to do so (Article 4(10) of the Regulation; Section 3(22) of the Privacy Act);

recipient: the natural person or legal entity or organisation without legal personality, public authority, agency or another body, to which the personal data are disclosed or made available by the controller or processor, whether a third party or not. However, 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; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing (Article 4(9) of the Regulation; Section 3(28) of the Privacy Act);

data transfer: providing access to the data for a designated third party (Section 3(11) of the Privacy Act);

restriction of processing: blocking stored personal data with the aim of limiting their processing in the future (Article 4(3) of the Regulation);

profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4(4) of the Regulation);

pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4(5) of the Regulation);

consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them (Article 4(11) of the Regulation);

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 (Article 4(12) of the Regulation).

3. MANAGEMENT OF COOKIES

3.1. Purpose of data processing

During visits to the www.babolnatakarmany.hu website, the Controller uses so-called cookies (hereinafter the **cookies**). A cookie is an information package made up of letters and numbers, which is sent by the Controller's website to the browsers of users with the aim of saving certain settings, facilitating the use of the Controller's website and helping the Controller collect certain relevant information of statistical nature concerning users. Cookies do not contain personal information and are not suitable to identify individual users.

The purpose of data processing relating to cookies is to identify users, distinguish users from one another, identify the current session of users, the storage of data provided during such sessions, the prevention of data loss, obtaining information on browser specifications and to increase the efficiency of service. For the purpose of providing the service, controlling the operation of the service and preventing fraud and abuse, the Controller records visitor data that are technically indispensable for providing the service. Data generated during the analysis of log files are not linked to other information by the Controller, and the Controller does not attempt to identify the visitor.

Cookies often contain an individual identifier, i.e. a secret, randomly generated sequence of digits, that is stored on the user's computer. Some cookies expire after the browser is closed, while others are stored on the user's computer for longer periods.

3.2. Types and use of cookies

3.2.1. Cookies categorised by lifespan:

A. session cookies

'Session cookies' are automatically deleted when the user closes their browser.

B. persistent cookies

Whereas ‘persistent cookies’ remain stored in the user’s terminal device until a set expiration date (which can be minutes, days or several years in the future) or until they are deleted manually by the user.

3.2.2. Cookies categorised by place of origin:

A. first party cookies

The term "first party cookies" is used as reference to cookies that have been installed by the controller (or any of its processors) operating the website visited by the user as generally displayed in the browser address bar (URL).

B. third party cookies

“Third party cookies” are cookies that are set by a controller other than the operator of the website visited by the user (as displayed in the browser address bar (URL)).

3.2.3. Cookies categorised as defined by the Working Party on Data Protection:

A. Cookies exempted from consent (technically necessary cookies)

1. user-input cookies

The term “user input cookies” can be used as a generic term to describe session cookies that are used to keep track of the user’s input in a series of message exchanges with a service provider in a consistent manner. Such first party cookies typically rely on a Session ID (a random temporary unique number) and expire when the session ends at the latest.

First party “user input cookies” are typically used to keep track of the user’s input when filling in online forms over several pages, or as a shopping cart, to keep track of the items the user has selected by clicking on a button (e.g. “add to my shopping cart”). Such cookies are clearly needed to provide the Internet service expressly requested by the user. Additionally, they are linked to a user action (such as clicking on a button or filling in a form).

2. authentication cookies

Authentication cookies are used to identify the user once they have logged in (for example on an online banking website). These cookies are needed to allow users to identify themselves on successive visits to the website and gain access to authorised content, such as when checking their account balance, transactions, etc. Authentication cookies are usually session cookies. When a user logs in, they explicitly request access to the content or functionality to which they are authorised. Without the use of an authentication token stored in a cookie, the user would have to provide a username/password on each page request. Therefore this authentication functionality is an essential part of the information society service they are expressly requesting. However, it is important to note that the user is only requesting access to the site and specific functionality to perform the task they require. The act of authentification must not be taken as an opportunity to use the cookie for other secondary purposes such as behavioural monitoring or advertising without consent.

3. **user centric security cookies**

The exemption (as detailed above) that applies to authentication cookies can be extended to other cookies set for the specific task of increasing the security of the service that has been explicitly requested by the user. This is the case for example for cookies used to detect repeated failed login attempts on a website, or other similar mechanisms designed to protect the login system from abuses. However, this exemption shall not apply to the use of cookies that relate to the security of websites or third party services that have not been expressly requested by the user. While login cookies are typically set to expire at the end of a session, user security cookies are expected to have a longer lifespan to fulfil their security purpose.

4. **multimedia player session cookies**

Multimedia player session cookies are used to store technical data, such as image quality, network link speed and buffering parameters, needed to play back video or audio content. Such multimedia session cookies are commonly known as “flash cookies”, so called because the most prevalent internet video technology in use today is Adobe Flash. As there is no long-term need for such information, they should expire once the session ends. When the user visits a website containing related text and video contents, both of such contents are equally part of a service expressly requested by the user. Website operators must avoid the inclusion of additional information into the “flash” or other cookies which are not strictly necessary for the playback of the media content.

5. **load balancing session cookies**

Load balancing is a technique that allows distributing the processing of web server requests over a pool of machines instead of just one. One of the techniques that are used to achieve load balancing is based on a “load balancer”: web requests from the users are directed to a load balancing gateway which forwards the request to one of the available internal servers in the pool. In some cases, such redirection needs to be persistent during a session: all requests originating from a specific user must always be forwarded to the same server in the pool to maintain the consistency of the processing. Among several techniques, a cookie may be used to identify the server in the pool in order for the load balancer to redirect the requests appropriately. These are session cookies. The information in the cookie has the sole purpose of identifying one of the communication endpoints (one of the servers in the pool) and is thus necessary to carry out the communication over the network.

6. **user interface customisation cookies**

User interface customisation cookies are used to store a user’s preference regarding a service across web pages and not linked to other persistent identifiers such as a username. They are only set if the user has expressly requested the service to remember a certain piece of information, for example, by clicking on a button or ticking a box. They may be session cookies or have a lifespan counted in weeks or months, depending on their purpose.

Typical examples of **customisation cookies** are:

a) language preference cookies that are used to remember the language selected by a user on a multilingual website (e.g. by clicking on a “flag”);
b) result display preference cookies that are used to remember the user’s preference regarding online search queries (e.g. by selecting the number of results per page).

7. social plug-in consent sharing cookies

Many social networks offer “social plug-in modules” that website operators can integrate into their platform, notably to allow social network users to share contents they like with their “friends” (and propose other related functionalities such as publishing comments). Such plug-ins store and access cookies in the user’s terminal equipment in order to allow the social network to identify their members when they interact with such plug-ins. To address such issue of use, it is important to distinguish users who “logged-in” through their browser in a particular social network account, from “non-logged-in” users who are either simply not a member of that specific social network or who have “disconnected” from their social network account.

B. Cookies that do not require user consent (optional cookies)

1. social plug-in tracking cookies

Many social networks offer “social plug-in modules” that website owners can integrate into their platform, to provide some services than can be considered as “expressly requested” by their members. However, these modules can also be used to track individuals, both members and non-members, with third party cookies for additional purposes such as behavioural advertising, analytics or market research, for example.

2. third party advertising

This group includes third party cookies used for behavioural advertising, as well as all related third party operational cookies used in advertising including cookies used for the purpose of frequency capping, financial logging, ad affiliation, click fraud detection, research and market analysis, product improvement and debugging.

The Do Not Track (DNT) function is a browser-side opt-out settings option. If this function is turned on, by sending the Do Not Track header for each page request, the browser indicates to service providers (web analytics system, ad serving system, other providers) that providers may not store online behavioural data on the given user, i.e. no cookies may be placed on their computer. In essence, this results in an action similar to when the user had opted-out at the given service provider, but in this case a browser setting is used to signal all service providers that the user does not want their online browsing to be tracked. Therefore, where a user has expressed the preference to not be tracked (DNT=1) no identifier, for the purpose of tracking, may be set or otherwise processed.

3. first party analytics

Analytics are statistical audience measurement tools for websites, which often rely on cookies. These tools are notably used by website owners to estimate the number of individual visitors, to detect the most prominent search engine keywords that lead to a webpage or to track down website navigation issues.

3.2.4. Classification by the United Kingdom International Chamber of Commerce (ICC UK):

The most widely-used classification system of cookies today at least on English language websites, has been proposed and developed by the United Kingdom International Chamber of Commerce (ICC UK) in its document entitled ICC UK Cookie Guide:

A. strictly necessary cookies/necessary

These cookies are essential for the use of the website, and allow for the use of its functions and features. These include cookies to enable users to access secure areas of the website, use shopping baskets or e-billing services.

B. performance cookies/statistics

These cookies collect information about how visitors use a website, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies do not collect information that identifies a visitor. All the information such cookies collect is aggregated and therefore anonymous. They are only used to improve how a website works.

C. functionality cookies/preferences

These cookies allow the website to remember choices made by the user (such as user name, language or the region) and provide enhanced, more personal features. In addition, in the interest of appropriate operation, these cookies may enable certain functions embedded into the website (for example displaying YouTube videos).

The information these cookies collect may be anonymised and they cannot track browsing activity on other websites visited by the user.

D. targeting cookies or advertising cookies/marketing

The aim of these cookies is to deliver adverts more relevant to the user and their interests. They are also used to limit the number of times the user sees an advertisement as well as help measure the effectiveness of the advertising campaigns. They are usually placed by advertising networks with the website operator's permission. They remember visits to a website and this information is shared with other organisations, such as advertisers. Typically, targeting or advertising cookies will be linked to site functionality provided by the organisation operating the website.

E. unclassified cookies

Cookies that have yet to be classified have no classification, along with the providers of first party cookies.

3.3. Cookies most frequently used by the www.bonafarmcsoport.hu website

3.3.1. Strictly necessary cookies/necessary

Name	Provider	Purpose	Type	Expiry
PHPSESSID	bonafarmcsoport.hu	Preserves user session state across page requests.	HTTP	When the session ends.

3.3.2. Performance cookies/statistics

Name	Provider	Purpose	Type	Expiry
_utm.gif	google-analytics.com	Google Analytics Tracking Code that logs details about the visitor's browser and computer.	Pixel	When the session ends.
__utma	babolnatakarmany.hu	Collects data on the number of times a user has visited the website as well as dates for the first and most recent visit. Used by Google Analytics.	HTTP	2 years
__utmb	babolnatakarmany.hu	Registers a timestamp with the exact time of when the user accessed the website. Used by Google Analytics to calculate the duration of a website visit.	HTTP	1 day
__utmc	babolnatakarmany.hu	Registers a timestamp with the exact time of when the user leaves the website. Used by Google Analytics to calculate the duration of a website visit.	HTTP	When the session ends.
__utmt	babolnatakarmany.hu	Used to throttle the speed of requests to the server.	HTTP	1 day
__utmz	babolnatakarmany.hu	Collects data on where the user came from, what search engine was used, what link was clicked and what search term was used. Used by Google Analytics.	HTTP	6 months
_ga	babolnatakarmany.hu	Registers a unique ID that is used to generate statistical data on how the visitor uses the website.	HTTP	2 years
_gat	babolnatakarmany.hu	Used by Google Analytics to throttle request rate.	HTTP	1 day
_gid	babolnatakarmany.hu	Registers a unique ID that is used to generate statistical data on how the visitor uses the website.	HTTP	1 day
collect	google-analytics.com	Used to send data to Google Analytics about the visitor's device and behaviour. Tracks the	Pixel	When the session ends.

		visitor across devices and marketing channels.		

3.3.3. Targeting cookies or advertising cookies/marketing

Name	Provider	Purpose	Type	Expiry
GPS	youtube.com	Registers a unique ID on mobile devices to enable tracking based on geographical GPS location.	HTTP	1 day
IDE	doubleclick.net	Used by Google DoubleClick to register and report the website user's actions after viewing or clicking one of the advertiser's ads with the purpose of measuring the efficacy of an ad and to present targeted ads to the user.	HTTP	1 year
PREF	youtube.com	Registers a unique ID that is used by Google to keep statistics of how the visitor uses YouTube videos across different websites.	HTTP	8 months
test_cookie	doubleclick.net	Used to check if the user's browser supports cookies.	HTTP	1 day
VISITOR_INFO1_LIVE	youtube.com	Tries to estimate the users' bandwidth on pages with integrated YouTube videos.	HTTP	179 days
YSC	youtube.com	Registers a unique ID to keep statistics of what videos from YouTube the user has seen.	HTTP	When the session ends.
yt-remote-cast-installed	youtube.com	Stores the user's video player preferences using embedded YouTube video.	HTML	When the session ends.
yt-remote-connected-devices	youtube.com	Stores the user's video player preferences using embedded YouTube video.	HTML	A persistent cookie that is stored on the user’s terminal equipment until the defined expiration date or until deleted

				manually by the user.
yt-remote-device-id	youtube.com	Stores the user's video player preferences using embedded YouTube video.	HTML	A persistent cookie that is stored on the user's terminal equipment until the defined expiration date or until deleted manually by the user.
yt-remote-fast-check-period	youtube.com	Stores the user's video player preferences using embedded YouTube video.	HTML	When the session ends.
yt-remote-session-app	youtube.com	Stores the user's video player preferences using embedded YouTube video.	HTML	When the session ends.
yt-remote-session-name	youtube.com	Stores the user's video player preferences using embedded YouTube video.	HTML	When the session ends.

3.3.4. Unclassified cookies

Name	Provider	Purpose	Type	Expiry
Ho_BAilwK	bonafarmcsoport.hu	No classification.	HTTP	1 day
mVfyGIcKRHPzN	bonafarmcsoport.hu	No classification.	HTTP	1 day
SCdmAlvJafhgwzB	bonafarmcsoport.hu	No classification.	HTTP	1 day

3.4. Legal basis for data processing

Pursuant to **Article 6(1) a) of the Regulation, Article 2(5) of Directive 2009/136/EC , Section 155(4) of the Electronic Communications Act and Section 13/A(4) of the E-commerce Act**, the legal basis for processing shall be the consent of the data subject, and **Section 13/A (3) of the E-commerce Act** for cookies that require consent.

The consent granted regarding the use of cookies may be withdrawn or amended by the data subject at any time, in line with Section 3.8 of this Data Processing Notice.

3.5. Categories of data subjects

Data subjects shall mean visitors to the www.babolnatakarmany.hu website.

In the event of data processing required for the essential operation of the www.babolnatakarmany.hu website (strictly necessary cookies) and the security of the IT system (server logs, etc.), the categories of data subjects shall include visitors to the www.babolnatakarmany.hu website as well as administrators authorised to use the administration interface of the www.babolnatakarmany.hu website.

3.6. Categories of personal data processed

Processing necessary for the essential operation of the www.babolnatakarmany.hu website and the security of the IT system is performed by providing the following personal data, which are required for the operations below:

a) name: for identification;
b) password:

for secure login.

3.7. Duration of data processing

During processing necessary for the essential operation of the www.babolnatakarmany.hu website and the security of the IT system, the personal data provided in Section 3.6 are deleted at the end of the session.

3.8. Recipients and categories of recipients of personal data

a) Controller

The business association specified in Section1 of this Data Processing Notice.

b) Processor(s)

ba) István Róbert Bogdán, Sole Trader (mailing address: H-6710 Szeged, Palánta utca 8; email address: robert.bogdan02@gmail.com), as the sole trader in charge of website development.

bb) Invitech ICT Services Kft. (mailing address: H-2040 Budaörs, Edison utca 4; email address: fazekasb@invitech.hu; website: www.invitech.hu; telephone number: 1444), as the business association providing storage services.

3.9. Processing by third party providers

The HTML code of the portal may contain links from and to third party servers. The servers of third party service providers may be directly connected to the visitor's computer. Please be advised that the aforementioned service providers are capable to collect user data due to the direct communication with the user's browser. Contents that may be personalised for the visitor are served by servers of third party service providers. Cookies used by third party providers are primarily the **Google Adwords cookie**, the **Google Analytics cookie** or the cookies used by **Facebook**.

More information on cookies used by **Google** is available here:

https://policies.google.com/technologies/types?hl=hu

More information on cookies used by **Facebook** is available here:

https://hu-hu.facebook.com/policies/cookies/

3.10. Setting, deleting or blocking cookies

Users can delete cookies from their own computer or disable the use of cookies in the browser. If the visitor to the www.babolnatakarmany.hu website does not accept the use of cookies, certain functions and features

may not be available to them. If the visitor to the website wants to disable cookies in part or in full, they must do so individually on all devices and programmes suitable for browsing.

The settings for the cookies used by the www.babolnatakarmany.hu website may be viewed and changed by the visitor:

a) in case of the Firefox browser, by clicking the "Site Information" icon in front of the browser address bar (in the case of a secure connection – https – a padlock, in all other cases a circled letter "i"), in the pop-up window, or

b) in case of the Chrome browser, in the Settings/Advanced/Privacy and security/Content settings/Cookies menu.

More information on cookies is available here:

a) Microsoft Internet Explorer:
https://support.microsoft.com/en-gb/help/17479/windows-internet-explorer-11-change-security-privacy-settings

b) Firefox:
https://support.mozilla.org/hu/products/firefox/protect-your-privacy/cookies

c) Google Chrome:
https://support.google.com/accounts/answer/61416?hl=hu

d) Microsoft Edge
https://privacy.microsoft.com/hu-HU/windows-10-microsoft-edge-and-privacy

e) Opera
https://help.opera.com/en/latest/web-preferences/#cookies

f) Safari
https://www.apple.com/legal/privacy/en-ww/

4. SECURITY OF PROCESSING

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and the Processor(s) shall implement appropriate technical and organisational measures that ensure to data subjects a level of data security appropriate to the risk.

In assessing the appropriate level of security, account shall be taken by the Controller in particular of the risks that are presented by processing, in particular arising from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transferred, stored or otherwise processed.

The Controller and Processor(s) shall take steps to ensure that any natural person acting under the authority of the Controller and Processor(s) who has access to personal data does not process them except on instructions from the controller, unless they are required to do so by Union or Member State law.

Accordingly the Controller and the Processor(s) shall ensure:

a) physical security, including the physical protection of all elements of the IT infrastructure that are involved in serving the given service, the guarding of the facilities housing the systems, as well as the supervision and control of access to the premises;
b) logical security, which comprises the allocation of logical access to the given IT service based on the principle of least privilege, the supervision and control thereof, ensuring the confidentiality and integrity of the stored data;
c) the availability of systems, including ensuring the uninterrupted operation and continuity of service provision as specified in the SLA (Service Level Agreement);
d) to perform risk analyses, where potential internal and external risks that may arise in relation to data processing and data management are identified, such as the risk of unauthorised access;
e) the uninterrupted execution of backups, that ensure the maximum rate of data loss as specified in the agreement;
f) patch-management, which ensures the up-to-date status of the server of the service used (OS, Application backend, Database), thus minimising the risk of threats arising from the exploitation of vulnerabilities;
g) performing vulnerability tests, which test at least every two years whether the tasks recorded in patch-management have been duly and properly implemented, whether there are known vulnerabilities whose patching has not been implemented or only implemented in part;
h) escalation, that in the event of errors ensures the solution available in the shortest possible time.

5. EXERCISE AND ENFORCEMENT OF RIGHTS AND LEGAL REMEDY

Data subjects may exercise their below rights under the Regulation in respect of the above detailed nature of the various legal grounds.

5.1. Rights of the data subject

5.1.1. Transparent information

The Controller shall provide all information required in the Regulation in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for information addressed specifically to children. Information is provided by the Controller in writing or by other means, e.g. electronically, but upon request by the data subject the information may also be provided orally, provided that the identity of the data subject is proven by other means.

5.1.2. Right of access to own personal data

At the request of the data subject, the Controller provides information as to whether or not personal data concerning them are being processed. Where it is established that personal data are indeed processed, the data subject may request access to the personal data and the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients 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 the Supervisory Authority;
g) where personal data are not collected by the Controller directly 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;
i) where the data subject's personal data are transferred to a third country or to an international organisation by the Controller, the data subject shall have the right to be provided information relating to the transfer.

5.1.3. Rectification of inaccurate personal data

If the Controller processes inaccurate or incomplete personal data on the data subject, it shall rectify such data without undue delay after receipt of the data subject's request to this effect. The data subject also has the right to have incomplete personal data completed.

5.1.4. Right to erasure ('right to be forgotten')

The data subject has the right to request from the Controller the erasure of personal data concerning them without undue delay and request the Controller to comply with such request without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;
c) the lawfulness of processing is the legitimate interest of the Controller, to which the data subject objects and there are no overriding legitimate grounds for the processing;
d) the purpose of data processing is direct marketing, to which the data subject objects;
e) the personal data have been unlawfully processed by the Controller;
f) the personal data of the data subject have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller is subject;
g) the lawfulness of the processing of personal data by the Controller is based on consent granted by the guardian of a child, and/or
   ga) The person in question is the child's guardian, and the child in question is under the age of 16 as required to grant consent;
   gb) the person in question is the child who is over the age of 16 as required to grant consent.

The Controller may not erase personal data if processing is required on the following grounds:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing or for the performance of a task carried out in the public interest or in the exercise of official authority;
c) for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;
d) for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

e) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the data subject's right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;
f) for the establishment, exercise or defence of legal claims.

5.1.5. Right to restriction of processing

Upon the data subject's request, the Controller restricts processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject;
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;
d) the data subject objects to processing on the grounds that the Controller has named its legitimate interest as legal basis, but the data subject states that their interests override those of the Controller.

Where processing has been restricted upon request by the data subject, such personal data may, with the exception of storage, only be processed

a) with the data subject's consent, or
b) for the establishment, exercise or defence of legal claims, or
c) for the protection of the rights of another natural or legal person, or
d) for reasons of important public interest of the Union or of a Member State.

The Controller shall inform the data subject before lifting the restriction of processing.

5.1.6. Right to data portability

The data subject shall have the right to receive the personal data concerning them, which they have provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, where:

a) the processing is based on consent or a contract; and
b) the processing is carried out by automated means.

The data subject shall also have the right to have the personal data transmitted directly from one controller to another.

5.1.7. Right to object

The data subject has the right to object to processing, where

a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
b) processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, including profiling;
c) where the data subject objects to processing for direct marketing purposes, including profiling, provided it is linked to direct marketing.

In the case of processing based on legitimate interest as per the above subsection b), the data subject may not object to processing if the Controller demonstrates that

a) there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or
b) for the establishment, exercise or defence of legal claims.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes by the Controller.

5.1.8. Automated individual decision-making, including profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

The data subject may not exercise the above right if the decision:

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

In the above detailed subsection a) and c), the data subject may request human intervention, may express their point of view and lodge a complaint against the decision.

5.1.9. Withdrawal of consent

The data subject is only entitled to withdraw consent at any time in matters where processing is based on their consent. The withdrawal of consent shall not affect the lawfulness of any processing that was conducted based on the consent prior to its withdrawal. Prior to granting consent, the data subject shall be informed thereof by the Controller.

The declaration by the data subject withdrawing consent is only valid if the given processing is clearly identified.

5.2. Enforcement of rights, lodging complaints, legal remedy

5.2.1. Enforcement of rights

The above specified data processing rights may be exercised by the data subject via email sent to the Controller's email address or to the Controller’s registered office email address from the data subject’s identifiable email address, or by post in a letter signed by the data subject. The declaration by the data subject on the exercise of rights is only valid if the given processing is clearly identified. The Controller responds to requests submitted electronically in electronic form or in the manner specified by the data subject.

5.2.2. Lodging complaints

If the data subject considers that the processing of personal data relating to them infringes the provisions of the Regulation, the data subject have the right to lodge a complaint with the Supervisory Authority, in particular in the Member State of their habitual residence, place of work or place of the alleged infringement.

Within the territory of Hungary, complaints may be lodged with the National Authority For Data Protection and Freedom of Information (hereinafter the **NAIH**), as Supervisory Authority. Contact details of the NAIH:

Email: ugyfelszolgalat@naih.hu
Mailing address: H-1125 Budapest, Szilágyi Erzsébet fasor 22/c
Telephone: +36 (1) 391-1400
Website: www.naih.hu

The names and contact details of data protection authorities in the territory of the European Union are available at http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

5.2.3. Legal remedy

a) Judicial remedy against the Supervisory Authority

All data subjects have the right to an effective judicial remedy:
aa) against a legally binding decision of a supervisory authority concerning them, or
ab) where the Supervisory Authority does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.
Proceedings against the Supervisory Authority shall be brought before the courts of the Member State where the Supervisory Authority is established.

b) Judicial remedy against the Controller or Processor

The data subject is entitled to file for action with the courts against the Controller or Processor where they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data by the Controller or the Processor acting on its behalf or under its instructions in non-compliance with the mandatory legal act of the European Union.

Proceedings against the Controller or Processor shall be brought before the courts of the Member State where they are established. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has their habitual residence, unless the Controller or Processor is a public authority of a Member State acting in the exercise of its public powers.

Alternatively, such proceedings may also be brought before the courts in Hungary, before the court competent according to the data subject's habitual residence or place of stay.