
**NOTICE ON DATA PROCESSING
OF PERSONAL DATA,
RELATED TO THE BONAFARM GROUP'S SUPPLIER DATABASE**

**NOTICE ON DATA PROCESSING
OF PERSONAL DATA,
RELATED TO THE BONAFARM GROUP'S SUPPLIER DATABASE**

CHAPTERS:

1. INTRODUCTION
2. DEFINITIONS
3. THE PURPOSE, LEGAL BASIS AND DURATION OF DATA PROCESSING, THE SCOPE OF PERSONAL DATA PROCESSED
4. PERSONS ENTITLED TO ACQUAINT THEMSELVES WITH THE DATA, RECIPIENTS OF THE DATA
5. SECURITY OF PROCESSING
6. EXERCISE AND ENFORCEMENT OF RIGHTS AND LEGAL REMEDY

1. INTRODUCTION

This Notice is intended to provide information on the data processing of external persons (hereinafter **data subjects**), whose data are processed by the Bonafarm Co. (Registered office: 1123 Budapest, Alkotás utca 53., company registration number: 01-10-0464679) as data controller (hereinafter **Data controller**), - satisfying the personal data of natural persons of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Article 13 of Regulation 2016/679 of the European Parliament and of the Council (hereinafter: the **Regulation**) obligation – provides information of conditions and treatment of personal data processing to those business organisations (hereinafter referred to as “Suppliers”) who register to the Bonfarm Group Supplier Database, located at the official website, www.bonafarmcsoport.hu.

The procurement procedures carried out by the Bonafarm Group are open to companies who comply with the supplier requirements. The tendering processes are conducted on an electronic platform. The registration on www.bonafarmcsoport.hu/en/partners/, ensures the entry of companies to Bonafarm Group Supplier Database and through it provides possibility to get invited future tender issued by the Bonafarm Strategic Purchasing Group.

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 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: 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 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);

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);

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

erasure of data: making the data unrecognisable in a way that their recovery is no longer possible (Section 3(13) of the Privacy Act);

objection: statement by the data subject in which they object to the processing of their personal data and request the termination of data processing and the erasure of the data processed (Section 3(8) of the Privacy Act);

Regulation: 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).

3. THE SCOPE OF PERSONAL DATA PROCESSED, THE PURPOSE, LEGAL BASIS AND DURATION OF DATA PROCESSING

3.1. The scope of personal data processed

Name, telephone number and e-mail address of the contact person of the Data Provider

If there is a change in the data provided during the registration, the Data Controller will make the modification as Data Provider sends the request to the following email address: info@bonafarm.hu

3.2. The purpose of data processing

Ensuring registration in the Bonafarm Group's supplier database.

The purpose of the data management, is that companies register themselves on the Bonafarm Group website (www.bonafarmcsoport.hu) by completing the registration form under page "For our partners" and become included in the Bonafarm Group's supplier database in order get invitation to Group tenders that will be announced in the future.

3.3. The legal basis of data processing

The enforcement of the legitimate interests of the data controller and the contractual business partner pursuant to point (f) of Article 6 (1) of the Regulation. The registering party agrees to share its personal data according to the data set out in point 3.1. by filling the box next to the statement: " I have read the content of the data management information and I expressly agree to the processing of my personal data under the conditions contained therein" in the end of the registration form.

3.4. Duration of data processing

The Data controllers process the personal data indicated in point 3.1. till the data processing concerned (request of cancellation), but no later than 5 years from the date of registration. The registering party may send the request of cancellation in writing, electronically to the e-mail address info@bonafarm.hu. After receipt of the above statement or the expiry of the period of data processing, the Data controller deletes data from the Bonafarm Group's supplier database.

4. PERSONS ENTITLED TO ACQUAINT THEMSELVES WITH THE DATA, RECIPIENTS OF THE DATA

4.1. Data controller

Bonafarm Zrt. (Mailing address: 1123 Budapest, Alkotás utca 53., MOM PARK, Tower B, 4th floor; e-mail address: info@bonafarm.hu; website: www.bonafarmhmä.hu; telephone number: +36-1-801-9061) as business company providing IT and procurement services to the Data Processors listed in point 4.2. a) below, and the operator of the server that stores the personal informations.

4.2. Recipients of the data

Data processors:

- a) **Bonafarm Zrt.** (mailing address: 1123 Budapest, Alkotás utca 53., MOM PARK, B torony, IV. emelet; e-mail address: info@bonafarm.hu; website: www.bonafarmcsoport.hu; phone number: +36-1-801-9061)
- b) **Bonafarm-Bábolna Kft.**(mailing address: 2942 Nagyigmánd, Burgert Róbert Agrár-Ipari park 03/25 hrsz.; e-mail address: info@btakipar.hu; website: www.babolnatakarmany.hu; phone number: +36-34-557-062)
- c) **Bóly Zrt.** (mailing address: 7754 Bóly, Ady E u 21.; e-mail address: birosag.iratok@boly.bonafarm.hu; website:www.bonafarmcsoport.hu/bonafarm-csoport/boly-zrt; phone number: +36-69-57-0001)
- d) **Csányi Pincészet ZRT.**(mailing address: 7773 Villány, Ady fasor 2.; e-mail address: villany@csanyipince.hu; website: www.csanyipinceszet.hu; phone number: +36-72-492-141)
- e) **Dalmand Zrt.** (mailing address: H-7211 Dalmand, Felszabadulás u.42.; e-mail address: titkarsag@dalmand.bonafarm.hu; website: <http://www.bonafarmcsoport.hu/bonafarm-csoport/dalmand-zrt/>; phone number: +36-74-539-100)
- f) **Fiorács Kft .**(mailing address: H-2941 Ács, F ő u. 43.; e-mail address: info@fioracs.bonafarm.hu; website: www.bonafarmcsoport.hu/bonafarm-csoport/fioracs-kft; phone number: +36-34-385-677)
- g) **PICK SZEGED Zrt.** (mailing address: H-6725 Szeged, Szabadkai út 18.; e-mail address:birosag.iratok@boly.bonafarm.hu; website: www.pick.hu; phone number: +36-62-567-000)
- h) **Sole-MizoZrt.**(mailingaddress:6728Szeged,Budapestiút6.;e-mail address: solemizo@solemizo.bonafarm.hu; website: www.mizo.hu; phone number: +36-62-569-000)
- i) **Agroprodukt Zrt.** (mailing address: 8500 Pápa, Szent István út 12.; e-mail address: titkarsag@agroprodukttr.hu; website: www.bonafarmcsoport.hu/bonafarm-csoport/agroprodukt-zrt; phone number: +36-89-511-200)
- j) **MCS Vágóhíd Zrt.** (mailing address: 7700 Mohács, Pick Márk út 1.; e-mail address: mvagohid@gmail.com; website: www.mcs.hu; phone number: +36-69-887-651)
- k) **Invitech ICT Services Kft.** (mailing address: 2040 Budaörs, Edison utca 4.; e-mail address: fazekasb@invitech.hu; website: www.invitech.hu; phone number: 1444), as the website service provider of www.bonafarmcsoport.hu.

4.3. Persons entitled to acquaint themselves with the data

- the employees of Bonafarm Zrt. with strategic purchasing rights
- the IT support employees of Bonafarm Zrt. just that extent that they can perform necessary technical IT tasks
- the employees of Data Processors listed in point 4.2 with strategic purchasing rights
- the employees of Invitech ICT Services Kft. participating in the provision of hosting services

5. 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.

6. 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.

6.1. Rights of the data subject

6.1.1. 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.

6.1.2. 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

6.1.3. 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.

6.1.4. 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.

6.1.5. 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.

6.1.6. 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.

6.1.7. 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.

6.1.8. 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.

6.1.9. 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.

6.2. Enforcement of rights, lodging complaints, legal remedy

6.2.1. 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.

6.2.2. 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.

6.2.3. 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.