

**Privacy Notice**  
**on data processing regarding the screening of phishing e-mails**

**1. Joint data controllership (BARE International)**

1.1. Joint data controllers

BARE International Inc. and subsidiaries (according to [Appendix 2](#))  
“Controller” or Controllers” or “BARE International” hereafter;  
of which

**BARE International Hungary Limited Liability Company**

For headquarters and postal address click [HERE](#)

Company registration number: 01-09-962318

E-mail address: [dataprivacy@bareinternational.com](mailto:dataprivacy@bareinternational.com)

represents primarily the joint data controllers to the Data Subjects.

1.2. Data protection officer

In connection with joint data processing, the duties of the data protection officer are performed by the data protection officer of BARE International Hungary Kft.

**BARE International Hungary Kft.**

Data Protection Officer

E-mail address: [dataprivacy@bareinternational.com](mailto:dataprivacy@bareinternational.com)

For headquarters and postal address click [HERE](#)

(hereinafter together: **Controller**).

1.3. The Controllers carry out the processing jointly. All Controllers participate in the organization and operation of the processing and jointly determine the rules of the processing.

1.4. During joint data processing, BARE International Hungary Kft. performs the tasks related to the individual information of the Data Subjects and the exercise of their rights.

1.5. The Controllers have appointed BARE International Hungary Kft. as contact in connection with data protection issues related to joint data processing. Data protection issues can be addressed to the Controllers primarily at the following contact details:

**BARE International Hungary Kft.**

E-mail address: [dataprivacy@bareinternational.com](mailto:dataprivacy@bareinternational.com)

For headquarters and postal address click [HERE](#)

In addition, the Data Subject can indicate their needs and exercise their rights in relation to joint data processing to any Controller.

1.6. In the course of joint data processing, with regard to data transfers from the territory of the European Union to third countries, the Joint Controllers comply with the European Commission (EU) on the general contractual conditions for the transfer of personal data to third countries in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, the contract conditions defined by EXECUTIVE DECISION 2021/914 (June 4, 2021) are applied. The Controllers have put into effect the terms of the referenced general contract with respect to each other and comply with the conditions of application. The joint Controllers have agreed upon the additional conditions of joint data processing.

## **2. Legislation applied during data processing**

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (April 27, 2016) on the protection of natural persons with regard to the processing of personal data and on the free flow of such data, and on the repeal of Directive 95/46/EC (general data protection regulation); (The EU General Data Protection Regulation - The General Data Protection Regulation of the European Union), (hereinafter: GDPR).

## **3. Scope of this notice**

3.1. The scope of this notice applies to the data processing related to the screening of phishing e-mails sent to the Controller.

3.2. This data processing is carried out using AI-based software.

## **4. Data Subjects concerned by data processing**

- a) Employees of the Controller who report incoming suspected fraudulent e-mails, and
- b) natural person senders whose e-mails are suspected as fraudulent:

- natural persons who use a BARE e-mail account:
  - BARE employees,
  - freelancers,
  - contractors,
  
- natural persons who do not use a BARE e-mail account:
  - business partners and their contact persons,
  - customer contact persons,
  - senders of unsolicited e-mails,

hereinafter referred to as **Data Subject** or **Data Subjects**.

## 5. Temporal effect of this notice

This notice shall be effective from its date until the issuance of a new notice on the same subject.

## 6. Purpose of data processing

The purpose of data processing is to ensure a higher level of protection of the Controller's IT system against cyberattacks by AI-based analysis of suspected fraudulent e-mails received by the Controller.

## 7. Scope of processed data

The Data Subject's:

- e-mail address,
- name,
- content of their e-mail, particularly the domain names and URLs included in the e-mail,
- attachments and their contents,
- data in the e-mail signature (e.g. photo, phone number, address, represented organization, signature),

- metadata about the e-mail (time of sending or receiving the e-mail, recipients, size of e-mail attachments).

## **8. Legal basis for data processing**

8.1. The legal basis for data processing regarding the screening of phishing e-mails is the enforcement of the legitimate interest of the Controller pursuant to Article 6 (1) point f) of the GDPR.

8.2. Information on the results of the balancing of interests:

8.2.1. Identification of the legitimate interest of the Controller:

It is the legitimate interest of the Controller to provide the highest possible level of protection against cyberattacks to its internal IT systems, thereby ensuring the security of the data processed by the Controller, the protection of information related to the operation, economic situation and activities of the Controller, as well as the continuous operation of its IT systems. The examination of fraudulent e-mails with an AI tool - from the point of view of whether they may have a potentially harmful effect on the IT systems of the Controller and the Data Subjects using them - serves as an appropriate tool to ensure a more effective and thus higher level of protection.

8.2.2. Necessity of data processing:

Considering the Controller's e-mail traffic and the volume of e-mails, the appropriate level of protection cannot be ensured by human resources alone.

Considering the technical development of the age, the use of the most effective tools for this purpose is necessary and justified.

8.2.3. Impact of data processing on the Data Subject:

None of the Processors relevant to the data processing use the processed data for a purpose other than the one established in this notice, the processed data is not used by the Provider of the AI tool to develop its own AI-based software, so from this aspect the data processing has no impact on the Data Subject.

After the investigation has been conducted, the data that has been generated during the investigation will be anonymized or deleted after a maximum of 30 days. The data processing has no effect on the Data Subject.

In the case of a Data Subject who does not use a BARE e-mail account and sends an e-mail to the Controller as an external sender from outside of the organization of the Controller, if it

can be established in the course of the screening that the e-mail under investigation classifies as a "phishing" e-mail, i.e. a fraudulent e-mail, the sender of the e-mail will be affected by the data processing because their e-mail will be automatically ignored by the Controller for security reasons. Therefore, the Data Subjects falling into this category may be negatively affected by the data processing in a way that their e-mail will be ignored by the Controller.

With regard to Data Subjects who use BARE e-mail account and are within the scope of the Controller's organization in this respect, the data processing can only have a positive effect, since if it can be established that a fraudulent e-mail has arrived in their e-mail account, they become protected against the possible damage that the fraudulent e-mail could cause by detecting it in advance.

It can be stated that the impact of data processing on the given Data Subject may vary depending on the Data Subject type, however, overall it can be determined that it does not have an impact on the private lives of the Data Subjects since the data processing applies to work and business related e-mails, therefore it is unlikely to have a significant impact on the private lives of Data Subjects.

8.2.4. Guarantees that serve the protection of the rights and interests of the Data Subject and the proportionate limitation of rights:

The protection of the rights of the Data Subject and the proportionate restriction of rights are served, among other things, by the fact that the Processors relevant to the data processing do not use the data for their own purposes and for the development of their own services, and that the processed data is kept and handled by them in accordance with the purpose of data processing, for an appropriate period of time.

If the e-mail is classified as a fraudulent e-mail as a result of the investigation, the e-mail and any other data generated during the investigation will be deleted or anonymized within a maximum of 30 days from the end of the investigation.

If the result is negative, i.e. it can be established that the e-mail is not a phishing e-mail, it will be further processed in accordance with the provisions of the privacy notice of its subject, but further copies of it generated during the investigation and the result of the investigation will be deleted or anonymized within a maximum of 30 days from the end of the investigation.

The protection of the data will be ensured with a direct API connection, a secure data transfer solution between the Controller and the Processor.

The Data Subject has the right to object to the processing of their personal data. This right also serves to protect their rights and ensure that any restrictions placed on them are proportionate.

8.2.5. Comparison of interests:

It is in the fundamental and reasonable interest of the Controller to increase its effectiveness, to ensure its internal security, and thereby to ensure its economic interest. Examining the mass influx of e-mails the Controller reviews in the most efficient way – in this case, the examination by AI – proves to be the most appropriate tool. With this data processing, the Controller can filter out the suspected fraudulent e-mails it receives faster and more efficiently, thereby preventing their possible harmful effects faster and more efficiently (either in the Controller's internal systems or to third parties in business relations with the Controller), thereby helping to increase the efficiency of the Controller and ensure its economic interests.

The Data Subject's fundamental interest is the protection of their personal data and the free exercise of their right to self-determination, however, with regard to the fact that the scope of data affected by data processing is work related, the impact of data processing on the Data Subject and the applied guarantees that ensure the protection of the Data Subject's rights and interests, it can be concluded that data processing does not constitute an excessive interference in the Data Subject's private life.

8.2.6. In addition to complying with the guarantees explained above, the Controller deems the data processing related to the screening of e-mails suspected of fraud to be justified, necessary and proportionate in order to enforce its legitimate interest.

## **9. Duration of data processing**

If the e-mail is classified as a fraudulent e-mail as a result of the investigation, the e-mail and any other data generated during the investigation will be deleted or anonymized within a maximum of 30 days from the end of the investigation.

If the result is negative, i.e. it can be established that the e-mail is not a phishing e-mail, it will be further processed in accordance with the provisions of the privacy notice of its subject, but further copies of it generated during the investigation and the result of the investigation will be deleted or anonymized within a maximum of 30 days from the end of the investigation.

## **10. How and where the data is stored**

Electronically, in the IT system of the Controller and in the IT systems of the Service Provider Processors (recipients) used by the Controller. Further information about the Processors can be found in Chapter 12.

## 11. Persons entitled to access the data and the rules of access

The data may be accessed by the IT administrators employed by the Controller involved in the screening of the fraudulent e-mails.

## 12. Recipients (use of processors)

### 12.1. Scan for suspected fraudulent e-mails

12.1.1. Scope of Data Subjects: Data Subjects mentioned in this notice.

12.1.2. Controller uses the Service Provider of the software used to inspect e-mail messages:

#### **OpenAI LL.C**

company number: 20211548334

headquarters: 1455 3rd Street, San Francisco, CA 94158.

contact: help.openai.com

as Processor (hereinafter: **Processor**).

12.1.3. The purpose of using the Processor: to provide a higher level of protection of the Controller's IT system against cyberattacks by scanning suspicious e-mails using AI technology.

12.1.4. Data processed by the Processor: personal data mentioned in this notice.

12.1.5. Nature of data processing: electronically.

### 12.2. Scan URLs in suspected fraudulent e-mails (VirusTotal)

12.2.1. Scope of Data Subjects of data processing: if the URL or the content accessible on it contains personal data, then the Data Subject is the person who can be identified on the bases of such data.

12.2.2. Controller uses Service Provider of the scanner of suspicious e-mails:

**Hispasec Sistemas, S.L.**

NIF (tax no.): B92183938.  
Registered Office: C/ Severo Ochoa, 8, 29590 - Málaga (Spain).  
Telephone: 952 02 04 94.  
E-mail: [gdpr@hispasec.com](mailto:gdpr@hispasec.com)  
contact: <https://www.virustotal.com/gui/contact-us/other>  
as Processor (hereinafter: **Processor**).

12.2.3. The purpose of using the Processor: to provide a higher level of protection of the Controller's IT system against cyberattacks by examining URLs in suspicious e-mails.

12.2.4. Data processed by the Processor: URLs in e-mails suspected as fraudulent, if they or the content accessible through them contain personal data.

12.2.5. Nature of data processing: electronically.

12.3. Data processing in connection with the use of Microsoft software services

12.3.1. Scope of Data Subjects involved in data processing: Data Subjects indicated in this notice.

12.3.2. Controller uses Service Provider as the provider of electronic hosting and developer of software for e-mailing and Office applications (e.g. Outlook, SharePoint, LogicApp, etc.)

**Microsoft Ireland Operations Limited**

short name: Microsoft Ireland Ltd.  
reg. no.: 256796  
tax number: IE8256796U  
residence: 70 Sir Rogerson's Quay, Dublin 2, Ireland  
postal address: One Microsoft Place, South County Business Park,  
Leopardstown, Dublin 18, Ireland  
telephone: +1 800 710 200  
website: [www.microsoft.com](http://www.microsoft.com)  
as Processor (hereinafter: **Processor**).

12.3.3. Scope of data involved in data processing: first of all, the name and e-mail address of those concerned, secondly further data of those concerned that has been sent in e-mails and other documents.

12.3.4. Purpose of using data processor: to ensure the functioning of e-mails and Microsoft apps.

12.3.5. Method of data processing: electronically.

12.4. Data Processing in connection with the use of ticketing management software (Jira)

12.4.1. Scope of those involved in data processing: Data Subjects indicated in this notice.

12.4.2. Controller uses the particular entity of the Processor to provide the software necessary for the ticketing system used for internal communication purposes based on territorial division:

in relation to data processing within the European Union:

name: **Atlassian B.V.**  
headquarters: Singel 236 1016 AB Amsterdam, Netherlands  
mailing address: Singel 236 1016 AB Amsterdam, Netherlands  
e-mail: [eudatarep@atlassian.com](mailto:eudatarep@atlassian.com)

in relation to data processing outside the European Union:

name: **Atlassian Pty Ltd**  
headquarters: 350 Bush Street, Floor 13 San Francisco, CA 94104  
mailing address: 350 Bush Street, Floor 13 San Francisco, CA 94104  
e-mail: [privacy@atlassian.com](mailto:privacy@atlassian.com)  
as Processor (hereinafter: **Processor**).

12.4.3. Scope of data involved in the processing: personal data mentioned in this notice.

12.4.4. Purpose of using the Processor: the Controller uses the Processor to provide the software necessary for the ticketing system for internal communication purposes.

12.4.5. Method of data processing: electronically.

12.5. Add-on provider to scan e-mails (Infosec)

12.5.1. Scope of those involved in data processing: Data Subjects indicated in this notice.

12.5.2. Controller uses the Service Provider to provide the Outlook add-on to forward reported e-mails to a technical BARE mail box:

**Cengage Group**

registered address: 10650 Toebben Drive, Suite A, Independence, KY 41051,  
Delaware, United States

e-mail: [privacy@cengage.com](mailto:privacy@cengage.com)

website: <https://www.cengagegroup.com/>

as Processor, (hereinafter: **Processor**).

12.5.3. Scope of data involved in the processing: the Processor may necessarily have access to the personal data mentioned in this notice during the performance of the above tasks, but this does not necessarily occur. The purpose of the Processor's cooperation is not to use the data, but for technical reasons it may become necessary to carry out data processing operations.

12.5.4. Purpose of using the Processor: Controller uses the Processor to provide the software necessary to contribute during the scanning of fraudulent e-mails.

12.5.5. Method of data processing: electronically.

12.6. Controller uses no other data processors apart from those described above.

**13. Data protection, data security**

13.1. The Controller protects electronic data carriers with information security tools and measures appropriate at all times.

13.2. The Controller ensures the security of the data within the scope of its data management activities and ensures the enforcement of the law and other data protection and confidentiality rules with technical and organizational measures and internal procedural rules. In particular, it takes appropriate measures to protect the processed data against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as

against accidental destruction and damage or inaccessibility due to changes in the technology used.

13.3. The data is processed only in order to achieve the legitimate purposes described in this notice, to the extent necessary and proportionate, on the basis of the relevant laws and recommendations, with appropriate security measures.

13.4. In order to do so the Controller stores the processed data in the form of encrypted data files, separately for each data processing purpose, which can be accessed by certain employees of the Controller – performing tasks in the pursuit of the activities specified in this notice – whose job responsibilities are to protect the data and to handle them responsibly in accordance with this notice and the relevant laws.

13.5. The Controller also manages the electronically stored data with the softwares and in the systems of the IT service provider Processors specified in Chapter 12. The Controller has concluded a data processing contract with the Service Provider, in which the Processor undertook to guarantee data security in accordance with the GDPR and to the lawful processing of the data.

## **14. Data Subject's rights in relation to data processing**

### **14.1. Right to information**

14.1.1. By reading this Privacy Notice, the Data Subject gains information about the data processing at any time. At the request of the Data Subject, verbal information may also be provided, assured that the Data Subject's identity has been verified by other means. The Data Subject may request information both during and after data processing. The information covers all essential details of data processing and the way in which the Data Subject's rights can be exercised. At the request of the Data Subject, the Controller also informs the Data Subject about the measures taken on the basis of the Data Subject's requests – or the reason for their failure to do so, indicating the forums available for presenting a complaint.

14.1.2. Providing information is free of charge. If the Data Subject's request is clearly unfounded or excessive, especially because of its repetitive nature, the Controller, considering the administrative costs of providing the requested information or communication or taking the action requested, may:

- charge a reasonable fee, or
- refuse to take action on the basis of the request.

14.1.3. The Controller provides the information within the shortest possible time from the submission of the request (without undue delay), but no later than within one month.

#### 14.2. Right to access

14.2.1. The Data Subject has the right to access his or her data processed by the Controller. If requested to do so, the Controller informs the Data Subject whether data processing is in progress regarding to the Data Subject's personal data and as well about all the relevant circumstances related to the specific data processing.

14.2.2. According to the right of access, the Data Subject may request a copy of his/her personal data (including photo, and/or voice, and/or video recordings) processed by the Controller, which the Controller provides free of charge for the first time. For further copies, the Controller may charge a reasonable fee based on administrative costs.

14.2.3. The copy is provided by the Controller in a commonly used electronic format, unless the Data Subject requests otherwise.

14.2.4. If the Data Subject requests this, the Controller will provide him/her with written information about the data that's being processed of him/her.

14.2.5. The Controller provides access as soon as possible from the submission of the request (without undue delay), but no later than within one month.

#### 14.3. Right to rectification

14.3.1. The Data Subject has the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning the Data Subject.

14.3.2. Considering the purposes of data processing, the Data Subject is entitled to request the completion of incomplete personal data, including by means of providing a supplementary statement.

14.3.3. At the request of the Data Subject, the Controller rectifies or supplements where justified any inaccurate personal data concerning the Data Subject without undue delay.

#### 14.4. Right to erasure ("right to be forgotten")

14.4.1. The Data Subject has the right to obtain from the Controller the deletion of personal data concerning him or her without undue delay and the Controller is obliged to delete personal data related to the Data Subject without undue delay if one of the following reasons exist:

- a) personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
- b) the Data Subject withdraws consent on which the processing is based and there is no other legal basis for the processing;
- c) the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing subject to this notice, since in these cases the data processing is necessary for the enforcement of the legitimate interest of Controller);
- d) the personal data was unlawfully processed;
- e) the personal data must be erased in order to comply with a legal obligation imposed on the Controller by European Union or Member State law.

14.4.2. If Controller made personal data public – and according to cases mentioned above – has to erase them and must take reasonable steps, including technical ones – considering technology available and costs of realization – in order to inform Controllers involved about Data Subject requesting their personal data and the links referring to them or copies of personal data to be deleted.

14.4.3. The Controller is not obliged to delete the data necessary for the presentation, enforcement or protection of legal claims upon request by the Data Subject, nor is the Controller obliged to delete data processed for the protection of the vital interests of the Data Subject or another natural person or to fulfill an obligation under European Union or Member State law to which the Controller is subject. By default, however, after the retention period has expired, the Controller deletes the data without a request.

#### 14.5. Right to restriction of data processing

14.5.1. At the request of the Data Subject, the Controller restricts data processing in case one of the following conditions applies:

- a) the Data Subject contests the accuracy of the personal data, in which case the restriction applies to the period that allows the Controller to verify the accuracy of the personal data and any descriptions made of them;
- b) the processing is unlawful, and the Data Subject opposes the erasure of the data and instead requests the restriction of its use;

- c) the Controller no longer needs the personal data for the purpose of data processing, but the Data Subject requires them for the establishment, exercise or defence of legal claims;
- d) the Data Subject has objected to the processing; in this case, the restriction applies to the period until it is established whether the legitimate interests of the Controller override the legitimate interests of the Data Subject. Data Subject can object against data processing subject to this notice, since the data processing is necessary for the enforcement of the legitimate interest of Controller.

14.5.2. Where data processing has been restricted, such personal data will, with the exception of storage, only be processed with the consent of the Data Subject or for the presentation, enforcement or defense of legal claims or for the protection of the rights of another natural or legal person or for important public interest of the European Union or a Member State.

14.5.3. The Controller in advance informs the Data Subject - who has contested the accuracy of the personal data and based on this contest the data processing has been restricted - about the lifting of the restriction of data processing.

14.6. Notification obligation related to the rectification or deletion of personal data or restriction of processing

The Controller notifies the Data Subject about the rectification, restriction and deletion as well as all recipients to whom Data Subject's data have previously been transferred. Notification may be omitted if it proves impossible or requires a disproportionate amount of effort. At the request of the Data Subject, the Controller informs him or her about the recipients.

14.7. Right to data portability

14.7.1. The Data Subject has the right to receive the personal data concerning him/her that the Data Subject has provided to the Controller in a structured, commonly used and machine-readable format and has the right to transmit these data to another data controller without hindrance from the Controller to whom the Data Subject has made the personal data available, if:

- a) the processing is based on the consent of the Data Subject or on a contract concluded with them - this right cannot be practiced considering the legal basis of the data processing described in this notice.
- b) data processing is carried out by automated means.

14.7.2. When exercising the right to data portability as described above, the Data Subject has the right to have the personal data transmitted directly from one Controller to another, where technically feasible.

#### 14.8. Right to object

14.8.1. The Data Subject may object on grounds related to their particular situation, at any time to the processing of the Data Subject's personal data that's based on legitimate interest.

14.8.2. In this case, the Controller may further process the personal data only if it demonstrates compelling legitimate grounds for the data processing which override the interests, rights and freedoms of the Data Subject or for the submission, enforcement or defense of legal claims.

14.8.3. Data Subject can practice this right regarding data processing subject to this notice, since the data processing is necessary for the enforcement of the legitimate interest of Controller.

#### 14.9. Automated individual decision-making, including profiling

14.9.1. 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 him or her or similarly significantly affects him or her.

14.9.2. The Data Subject is entitled to this right regarding the data processing discussed in this present privacy notice and in order to exercise it he or she may submit their requests at Controller's contact details.

### 15. Fulfilling Data Subject's requests

15.1. During joint data processing, BARE International Hungary Kft. performs the tasks related to informing the interested parties and exercising their rights.

15.2. The Controller ensures notification and taking actions for free, as described in Chapter 14. If Data Subject's request is obviously unfounded, or especially for its repetitive nature, exaggerated, the Controller:

- a) might charge a reasonable price, or

- b) might deny taking actions based on request, considering data requested, or administrative costs of measures to be taken to fulfil request.

15.3. The Controller informs the Data Subject without any unreasonable delay, but maximum one month after receiving the request about actions that has been taken, including issuing copies of data. If necessary, considering the complexity of request and numbers of requests this deadline can be made longer with additional two months.

15.4. The Controller informs Data Subject about elongation of deadline along with indicating reasons for delay within one month of receiving the request. If the concerned Data Subject sends their request electronically, the Controller provides information electronically, except when concerned Data Subject asks for it in a different way.

15.5. If the Controller does not take any steps as reaction to Data Subject's request without delay but within maximum of one month after receiving the request, the Controller informs Data Subject about reasons why there have been no actions taken, and about the possibility of filing a complaint to the data protection authority competent in their place of residence and can have the right to legal remedy.

15.6. The Data Subject can hand in their request to the Controller in any way that identifies them. BARE International requests that the Data Subject provides their registered e-mail address in the request. A request is still valid if the registered e-mail address is not provided. Identifying Data Subjects who hand in a request is necessary because the Controller can deal with only those requests that are entitled. If Controller has justified doubts about the identity of the natural person handing a request, it can ask for other pieces of information to assure the identity of the Data Subject concerned.

15.7. Data Subject can send their requests to the Controller to the address included in [Annex 1](#) or to the e-mail address [dataprivacy@bareinternational.com](mailto:dataprivacy@bareinternational.com). The Controller considers request sent in e-mail as genuine, only if it was sent from an e-mail address registered in the Controller's database. However, the usage of a different e-mail address does not result in such request being disregarded. Time of receiving e-mails is the first day after the e-mail was sent.

## **16. Prosecution of rights**

16.1. The Joint Data Controller have appointed BARE International Hungary Kft. as the contact in connection with data protection issues related to joint data processing. Data protection issues can be addressed to the Joint Data Controller primarily at the following contact details:

**BARE International Hungary Kft.**

E-mail address: [dataprivacy@barienternational.com](mailto:dataprivacy@barienternational.com)

Postal address: as per [Annex 1](#)

In addition, the Data Subject can indicate his/her needs and exercise his/her rights in relation to joint data processing to any Controller.

16.2. Data Subject can contact the Controller with any complaints regarding the handling of Data Subject's data, also at the above contact details.

16.3. Those concerned Data Subjects may exercise their legal rights in court, or at the competent authority as follows:

- Data Subjects residing outside the EU may apply to the state body responsible for data protection according to their nationality;
- Data Subjects residing in the EU may apply to the Data Protection Authority operating in the Member State of their place of residence within the EU;
- All Data Subjects without differentiation based on their residence may apply to the Data Protection Authority residing at the seat or area of operation of the appointed Controller.

Among themselves, the Joint Data Controller has appointed BARE International Hungary Kft. to handle data protection issues. Data protection authority according to the place of operation of the appointed data controller:

**National Authority for Data Protection and Freedom of Information**

(Nemzeti Adatvédelmi és Információszabadság Hatóság)

Address: 9-11. Falk Miksa Street, Budapest 1055, Hungary

Postal address: P.O. Box 9 Budapest 1363, Hungary

Telephone: +36 1 391 1400

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

Website: <http://www.naih.hu/>

In case of choosing a process involving a courthouse, the lawsuit based on concerned Data Subject's choice can be initiated at the court in concerned person's residence or place of stay.

**BARE International**