PRIVACY NOTICE

Index Middle East FZE (hereinafter: **Data Controller**), as the operator of the **„Insp-Ex" application** (hereinafter: **Application**), hereby publishes the information on data processing within the framework of the Application and the services related to the Application.

By connecting to the Application, users visiting the Application (hereinafter: **User**) accept all terms and conditions included in this Privacy Notice (hereinafter: **Notice**) and therefore you are requested to carefully read this Notice and the Terms and Conditions before using the Application.

1.) DATA CONTROLLER'S DATA

The data controller is Index Middle East FZE.

Registered office:	UAE, Umm Al Quwain Business Center, Al Shmookh Building, UAQ Free Trade Zone
Postal address:	Veress Árpád, HU-1154 Budapest, Kozák tér 13-16.
E-mail address:	veress@ind-ex.ae
Phone:	+971565682854
Reg. Nr.:	3488

2.) PROCESSED DATA

a.) During registration

The User may provide their data on the registration interface in order to be able to use the services of the Application (hereinafter: **Registration**). During Registration the **following personal data must be provided** (all data marked with an * must be provided):

- full name*;
- e-mail address*;
- password*.

b.) User Account

Following registration, the system creates the User Account of the User, containing the following data and information:

- User's data provided during Registration.
- data provided during the use of the Application.

During the use of the User Account, the User can use the free and paid services of the Data Controller, modify the entered data, delete the data, except for the mandatory data.

During the use of the User Account, it is possible to provide the following data and information in order to ensure that these are properly included in the prepared documents and reports.:

- phone number;
- company name;
- position;
- documents to certify the competence;
- company logo.

c.) Complaint handling

In case that the User has a problem or complaint while using the Application or using the services available in the Application, he / she may contact the Data Controller at the contact details provided in this Notice and the Terms of Use. During the complaint handling, - in case of User is consumer pursuant to the relevant law – the following personal data must be provided:

- in case of a written complaint:
  - name;
  - postal address or e-mail address;
  - subject and content of the complaint.

- in the case of a verbal complaint or a verbal complaint communicated by telephone, if the complaint could not be remedied immediately, the Data Controller shall take a minute containing the following information:
  - name;
  - address;
  - place, date, method, subject and content of the complaint;
  - individual ID of the complaint.

Only persons aged over 18 may provide data on the Application.

3.) PURPOSE AND DURATION OF DATA PROCESSING

The Data Controller uses the data for the following purposes in relation to the supply of services available through the Application:

- *In the course of Registration on, and use of, the Application, use of the User Account:* The purpose of data processing to provide the services of the Application, such as the registration and fulfilment of the contract concluded for the purpose of the service, to contact with the Users in connection with the services; the management, modification, deletion of data stored in the User Account.
- *In the case of complaint handling:* The purpose of data processing is to handle complaints received by the Data Controller verbally, by phone, in writing and via e-mail from the User as consumer, and to document the User's identity, the exact time of the complaint and the content of the complaint, as well as the Data Controller's information about the complaint for the purpose of retrieval.

The Data Controller shall process the personal data during the existence of the purpose of the data processing or for the period prescribed by law as the following.

In the case of the Registration and using of User Account data are processed until the User requests the erasure of the data or withdraws the consent to the processing of their personal data, except for the data for the processing of which the Data Controller is obliged by law as set forth in the following paragraph.

In the case of service submitted through the Application, the Data Controller processes the necessary data in accordance with Section 6:22 of Act V of 2013 on the Civil Code in order to enforce the obligations and rights arising from the contract concluded between the User and the Data Controller for 5 (five) years after the purchase. Furthermore, pursuant to Section 169 of Act C on Accounting

(hereinafter: Accounting Act), the Data Controller shall retain the name and address of the User on the accounting document for 8 years, solely for the purpose of fulfilling the accounting obligation.

In the case of complaint handling, the Data Controller is obliged to retain the report on the verbal complaint, the written complaint and the answer to it for 3 (three) years pursuant to Section 17/A of Act CLV of 1997 on Consumer Protection.

The personal data shall be erased immediately when the purpose of data processes ceases to exist, after the expiry of the deadline indicated in this section, or at the request of the User.

4.) LEGAL GROUND OF PROCESSING PERSONAL DATA

In the course of Registration, using the User Account Users consent to the processing of their personal data by the Data Controller in compliance with this Notice. Processing of personal data is based on the voluntary and explicit consent of the User granted being aware of this Notice. The User has the right to withdraw their voluntary consent at any time.

With regard to personal data processed during the services, the legal ground for data processing is the performance of the contract concluded between the User and the Data Controller, the enforcement of the rights and obligations arising from the contract pursuant to Article 6 (1) e) of the GDPR. The legal ground for data processing related to an accounting document is the statutory provision ordering mandatory data processing, i.e., Section 169 of the Accounting Act.

In the case of complaint handling, the legal ground for data processing is Section 17/A of the Act CLV of 1997 on Consumer Protection.

5.) PARTIES ELIGIBLE FOR ACCESSING PERSONAL DATA, DATA PROCESSING

The Data Controller is entitled to have access to personal data in compliance with the provisions of effective laws and regulations.

The Data Controller does not apply any data processor regarding data processing but it reserves the right to involve data processors in the future, and to inform the Users about it by amending this Notice.

Without an expressed statutory provision, the Data Controller may transfer to third parties data suitable for personal identification only with the explicit consent of the particular user.

6.) USER RIGHTS

Access to personal data

Upon the request of the User, the Data Controller shall provide information on whether or not their personal data are being processed by the Data Controller, and where that is the case, shall grant them access to the personal data, and shares the following information:

- the purpose(s) of the processing;
- the categories of personal data concerned;
- the legal ground and recipient(s) in the event of transferring the personal data of the User;
- the envisaged processing period;
- the User's rights relating to the rectification, erasure and restriction of processing of the personal data, as well as the option to object to personal data processing;

- the possibility of lodging a complaint with a supervisory Authority;
- the data source;
- relevant information on profiling;
- the name, address of the processors and their activities related to data processing.

The Data Controller shall provide the User with a copy of the personal data undergoing processing free of charge. For any further copies requested by the User, the Data Controller may charge a reasonable fee based on administrative costs. Where the User makes the request by electronic means, the information shall be provided in a commonly used electronic form, unless otherwise requested by the data subject.

The Data Controller is obliged to provide the information at the request of the User in an intelligible form without undue delay, but no later than within one month from the submission of the request. The User may submit their request for access through the contact channels specified in Section 1.

Rectification of processed data

The User may request the Data Controller (at the contact details specified in Section 1) to rectify inaccurate personal data or the supplementation of incomplete data, taking into account the purpose of data processing. The Data Controller shall fulfil the rectification requirement without undue delay.

Erasure of processed data (right to be forgotten)

The User may request the Data Controller to erase their personal data without undue delay, the Data Controller shall be obliged to erase the personal data concerning the data subject without undue delay, if any of the following criteria is fulfilled:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the User withdraws its consent and here is no other legal ground for the processing;
c) the User objects to the processing of your personal data;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data obtained based on consent was collected with the provision of services relating to the information society to children.

Where the Data Controller has made the personal data public (made it available to a third party) and are obliged to erase them pursuant to the above, the Data Controller shall take into account the available technology and the cost of implementation, shall take reasonable steps to inform data controllers who are processing the affected personal data that the User has requested them to erase any links to, or copy or replication of those personal data, as well as to erase any duplicate copies.

Personal data are not required to be erased when data processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously

impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

Restriction of processing

The User has the right to request the Data Controller to restrict the data processing instead of rectifying or erasing personal data if any of the following criteria applies:

- the accuracy of the personal data is contested by the User, in which case the restriction applies for a period enabling the Data Controller to verify the accuracy of the personal data;
- the processing is unlawful and the User opposes the erasure of the personal data and requests the restriction of their use instead;
- the Data Controller no longer needs the personal data for the purposes of the processing, but the they are required by the user for the establishment, exercise or defence of legal claims;
- the User objected to data processing; in such cases the restriction shall only apply to the time period necessary to determine whether the legitimate reasons of the Data Controller override those of the data subject.

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

The Data Controller shall inform the User, at whose request the processing has been restricted, of the lifting of the processing restriction in advance.

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Data Controller communicates any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. At the request of the User, the Data Controller informs the User about these recipients.

Right to objection

The User has the right to object to the processing of their personal data, if the data 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 Data Controller;
- is necessary for the enforcement of the legitimate interests of the Data Controller or a third party.
- is based on profiling.

In the event of the User’s objection, the Data Controller shall abandon the processing of the personal data unless the Data Controller proves that the data processing is justified by compelling legitimate grounds which override the User’s interests, rights and freedoms, or are necessary for the establishment, exercise or defence of legal claims.

Measures of the Data Controller in case of the User's request

The Data Controller shall inform the User without undue delay, but no later than within one month

from the receipt of the request, of the measures taken in relation to the access, rectification, erasure, restriction, objection or data portability request. This deadline may, however, be extended by two months if warranted by the complexity of the request or the number of requests. The Data Controller shall notify the User of any such extension within one month of receiving the request; such a notification shall include the reason of the extension. If the User submits the request via an electronic channel, the notification shall preferably be sent to them in an electronic format unless the data subject requests a different format.

If the Data Controller fails to act upon the User's request they shall notify the User, without delay but no later than within one month of receiving the request, of the reasons of such a failure, and shall also inform the User that they may place a complaint at a supervisory authority, and may seek judicial legal remedy.

Upon the request of the User, the information, notifications and the measures taken on their request shall be provided free of charge. If the User's request is clearly unfounded or excessive, in particular because of its repetitive nature, the Data Controller may, either charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested or may refuse to take action in relation to the request. The burden of demonstrating the clearly unfounded or excessive nature of the request falls on the Data Controller.

7.) Managing and reporting of personal data breaches

All incidents are considered personal data breaches which result in the unauthorised processing or controlling of personal data, in particular unauthorised or accidental access, alteration, disclosure, erasure, loss or destruction of personal data processed, transferred, stored or processed by the Data Controller, or in its accidental destruction or damage.

The Data Controller is obliged to notify the NADPFI of the personal data breach without undue delay, but no later than 72 hours after the detection of the personal data breach, unless, the Data Controller can prove that the personal data breach is unlikely to pose a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay. The notification to NADPFI includes at least the following information:

- the nature of the personal data breach, the number and categories of data subjects and personal data;
- Title and contact information of the Data Controller;
- the likely consequences arising from the personal data breach;
- the measures taken or planned to manage, rectify or remedy the personal data breach.

The Data Controller shall inform the data subjects about the personal data breach via the Data Controller's Application within 72 hours after having become aware of the data breach. The information shall include at least the data specified in this Section.

The Data Controller keeps a record of each personal data breach for controlling the measures taken in relation to the occurring incidents and for providing information to the data subjects. The records contain the following data:

- the scope of the affected personal data;
- the range and number of data subjects;
- the date and time of the personal data breach;

- the circumstances and effects of the personal data breach;
- the measures taken for the prevention of the personal data breach.

The Data Controller keeps the data contained in the record for 5 years from the detection of a personal data breach.

8.) Data security

The Data Controller undertakes to ensure the security of data and takes all technical and organisational measures, puts into place the procedural rules that ensure the protection of all collected, stored and processed data, as well as preventing the destruction, unlawful use and unlawful alteration of data. The Data Controller also undertakes to call upon each third party to whom data are transferred or transmitted without the Users' consent to comply with the data security requirements.

The Data Controller shall ensure that no unauthorised persons may access, disclose, transfer, modify or erase the processed data. The processed data may be accessed only by the Data Controller and its employees, as well as the Processor employed by them, and the Data Controller shall not transfer the data to any third party not authorised to have access to them.

The Controller shall take every possible effort to ensure data are not accidentally damaged or destroyed. The Data Controller requires all its employees taking part in data processing activities to assume the above obligations.

The User acknowledges and accepts that in case their personal data are provided on the Application, full data protection cannot be guaranteed on the internet despite the fact that the Data Controller has up-to-date security equipment to prevent any unauthorised access to data or the detection thereof. If data are accessed without authorisation or data are obtained despite our efforts, the Data Controller shall not be held liable for the obtaining of data in such a manner or for any unauthorised access to them, or for any damage occurring at the User as a consequence thereof. In addition, the User may also supply personal data to third parties who may use them for unlawful purposes and in an unlawful manner.

9.) Law enforcement options

The Data Controller shall take all reasonable efforts to process personal data in compliance with the laws and regulations, however, if Users feel that this has not been complied with, they can write using the contact details indicated in Section 1.

If Users feel that their right to the protection of personal data has been violated, they can seek legal remedy in compliance with the applicable laws and regulations at the agencies that have jurisdiction, as

- the Hungarian National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11.; www.naih.hu; ugyfelszolgalat@naih.hu) or
- in court.

10.) Other provisions

This Policy is governed especially by the provisions of Act CXII of 2011 on the Right of Informational Self-determination and Freedom of Information and by the Hungarian law and the Regulation of the European Parliament and of the Council (EU) 2016/679 (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.

Budapest, 2021

…
Data Controller