PRIVACY NOTICE FOR CANDIDATES

The date of entry into force of this Privacy Notice: 17.12.2021

Controller's name: **KELER Central Depository Ltd.** (hereinafter: "**Controller**").

Detailed information relating to the Controller

Company (institution) name: KELER Central Depository Ltd.
Registered office: H-1074 Budapest, Rákóczi út 70-72.,
Email: keler@keler.hu
Website: https://www.keler.hu
Name and email address of the Data Protection Officer:
Dr. András Balázs Bordás, adatvedelmitisztviselo@keler.hu

Regarding the processing of your personal data the Controller hereby informs you (hereinafter: "**You**" or "**Data Subject**") of the principles and practices applied by it during the processing of such personal data and of your rights related to processing and the method of and opportunities for exercising such rights.

The Controller pays special attention to the fact that the personal data obtained by it during its operation and thereafter processed by it are processed and stored in accordance with the provisions of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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) (hereinafter: "**Regulation**").

Important information: You may ask for detailed information at any time on the processing of your data and may object to such processing. Additional information on such rights is available in Sections 2.1 and 2.6.

1. DATA PROCESSING SITUATIONS

1.1. PROCESSING RELATED TO THE SELECTION PROCESS

Processed data: personal data included in the candidate's CV and cover letter (typically: name, photo, age, qualification, professional experience, email address, phone number).

The purpose of processing: completing the selection process and establishing a legal relationship (typically: employment) with the most suitable candidate.

Legal basis for processing: the Data Subject's consent as per point (a) of Article 6(1) of the Regulation.

Description of the Controller's legitimate interest (if the legal basis is legitimate interest): -

Duration of processing: a period of one year from occupying the position.

Is the Data Subject obliged to provide the data? Is the provision of personal data a statutory or contractual requirement? What are the possible consequences of the failure to provide such data for You?: no such obligation exists.

Where data have not been obtained from the Data Subject, the source of personal data (are the data obtained from a publicly available source?): recruitment partner.

Are the data transferred to countries outside the EU? If yes, the adequacy decision or any other appropriate and suitable safeguard shall be indicated: no.

Is automated decision-making applied?: no.

Processors: recruitment partner.

1.2. PROCESSING RELATED TO HUMAN RISK DUE DILIGENCE

Processed data:
(i) name; name at birth; place (country, city) and date of birth; tax identification number; personal identification number; identifier of a foreign private person; mother's name; residential address (country, postal code, city, street, number); postal address (country, postal code, city, street, number); email address; citizenship; mobile phone number;
(ii) data related to the Data Subject's positions and ownership interest held at business associations; data as to whether the Data Subject has been a member or executive officer of a company which ceased to exist due to insolvency; data as to whether there are or were disciplinary proceedings initiated against the Data Subject for breach of duties or infringement of the law as well as the result thereof; membership in criminal organisations; opposing secret service relations;

The purpose of processing: KELER Ltd., as a system operator designated by the Central Bank of Hungary as per Section 9 of Act XXIII of 2003, was designated as a national critical system element[1] in 2016. Due to its activity and its key role in national economy, KELER Ltd. has increased interest in selecting the most appropriate employees also in terms of security.

The purpose of processing is to

- analyse reliability and behaviour, and
- identify any relations with criminal organisations or opposing secret services.

Legal basis for processing: legitimate interest (point (f) of Article (6)1 of the Regulation).

Description of the Controller's legitimate interest (if the legal basis is legitimate interest): the legitimate interest of the Controller, as a controller qualifying as a critical system element, as per point (f) of Article 6(1) of the GDPR in confirming that the reliability and integrity of the employee to be employed in the smooth performance of its activity specified by law are beyond any doubt.

Duration of processing: in the case of successful job application, the data are processed until the termination of the employment; in the case of unsuccessful job application, the processed personal data shall be erased without delay.

Is the Data Subject obliged to provide the data? Is the provision of personal data a statutory or contractual requirement? What are the possible consequences of the failure to provide such data for You?: if you fail to provide the data specified in point 1 of the above "Processed data" paragraph, the investigation concerning human risk cannot be conducted in full and the Data Subject cannot be employed. It is not mandatory to provide the data specified in point 2 of the above "Processed data" paragraph; failure to provide such data does not mean an obstacle to conducting human risk due diligence.

Where data have not been obtained from the Data Subject, the source of personal data (are the data obtained from a publicly available source?): open-source databases (register of companies), prior personal statement, Constitution Protection Office, other public registers, print media and media platforms and publicly available data on social networking sites.

Recipients, categories of recipients if there is data transfer: MNB-Biztonsági Zrt., in justified cases investigating authorities or the Constitution Protection Office.

Are the data transferred to countries outside the EU? If yes, the adequacy decision or any other appropriate and suitable safeguard shall be indicated: no.

Is automated decision-making applied?: no.

Processors: MNB-Biztonsági Zrt.

[1] Point (j) of Section 1 and Section 20 of Annex 1 of Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities, and Section 27 of Annex 3 of Government Decree No. 65/2013 (III.8.) on the implementation of Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities

Additional characteristics of processing:

MNB-Biztonsági Zrt. may prepare a study of the surroundings based on the public information available in the Data Subject's residential area or place of abode if significant risks arise preliminarily.

During processing, MNB-Biztonsági Zrt. does not perform secret information collection; it performs the tasks related to human risk management and provides an expert opinion on the candidate concerned exclusively based on the analysis of public data.

During the performance of the tasks specified in the contract, the Agent may perform any processing exclusively in KELER's IT system, including in particular the candidates' personal data.

With regard to the fact that the processing pursuant to this Notice may implement profiling[2] as per Article 4(4) of the GDPR, KELER Group, complying with point (a) of Article 35(3) of the GDPR, carried out the impact assessment as per Article 35(1) of the GDPR.

Result of the impact assessment:
During the impact assessment it was established that processing may involve significant risks concerning the Data Subjects, in particular as a result of profiling performed during human risk assessment; however, the strict organisational and technical measures applied by the Controller and the Processor prove to be sufficient to reduce the risks to an appropriate level. The Controller, as a critical system element, has key interest in confirming that the reliability and integrity of the employee to be employed in the smooth performance of its activity specified by law are beyond any doubt. As processing is necessary for the purposes of the legitimate interests pursued by the Controller and such interests are not overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, the data specified above may be processed by the Controller pursuant to point (f) of Article 6(1) of the GDPR.

[2] "profiling": means 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

2. YOUR RIGHTS AND AVAILABLE LEGAL REMEDIES

In relation to the above processing activities You as a data subject are entitled to the following rights and may enforce such rights as follows:

You are entitled, at any time, to request information regarding the data relating to You and processed by the Controller, to request the rectification, erasure and blocking of your data recorded and have the incomplete data completed, to exercise the right to data portability and of access to your personal data and to object to the processing of your personal data.

You may submit your request for exercising the rights specified in the previous paragraph primarily to the Data Protection Officer.

2.1. INFORMATION AND ACCESS TO PERSONAL DATA

Via the contact details set out in the above section, You may request the following information in writing from the Controller as to the processing performed by it:

- what personal data are processed,
- the legal basis for processing,
- the purpose of processing,
- the source of data,
- the duration of processing,
- to whom, when, based on what law, to which personal data the Controller provided access or to whom it transferred the personal data.

The Controller makes the data available to You in a commonly used electronic format unless You request the data in writing in a printed form. The Controller will not provide verbal information either via phone or in person.

The Controller provides you with the copy of personal data (in person at the Customer Service) free of charge for the first time. For additional copies requested by You, the Controller may charge a reasonable fee based on administrative costs. If You request the copy in electronic format, the Controller will provide You with the information via email in a commonly used electronic format unless otherwise requested by You.

If, after being informed, You do not agree with the processing and the accuracy of the data processed, as per those set out in this Section 2 You are entitled to request the rectification, completion or erasure of the personal data relating to You, the restriction of processing thereof and to object to the processing of such personal data, or to initiate the proceedings set out in Section 2.10.

2.2. THE RIGHT TO RECTIFICATION OF THE PERSONAL DATA PROCESSED AND TO HAVE SUCH DATA COMPLETED

Upon your written request the Controller shall, without undue delay, rectify the inaccurate personal data indicated by You, and complete the incomplete data with the content indicated by You. The Controller shall communicate any rectification or completion of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Controller shall inform You about the data of those recipients if You request it in writing.

2.3. RIGHT TO RESTRICTION OF PROCESSING

By submitting a written request You shall have the right to obtain from the Controller restriction of processing if

- the accuracy of the personal data is contested by You, for a period enabling the Controller to verify the accuracy of the personal data,
- the processing is unlawful and You oppose the erasure of the personal data and request the restriction of their use instead,
- the Controller no longer needs the personal data for the purposes of the processing, but they are required by You for the establishment, exercise or defence of legal claims,
- You object to processing pending the verification whether the legitimate interests of the Controller override your rights to protect your personal data.

Personal data subject to restriction shall, with the exception of storage, only be processed during such period with your 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. You will be informed by the Controller before the restriction of processing is lifted.

2.4. RIGHT TO ERASURE ("RIGHT TO BE FORGOTTEN")

You shall have the right to obtain from the Controller the erasure of personal data concerning You 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 by the Controller;
b) You withdraw consent on which the processing is based and where there is no other legal ground for the processing;
c) You object, on grounds relating to your particular situation, to processing, and there are no overriding legitimate grounds for the processing;
d) You object to processing of personal data concerning You for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing;

e) the personal data have been unlawfully processed by the Controller;
f) the personal data have been collected in relation to the offer of information society services directly to a child.

You shall not be entitled to exercise your right to erasure ("right to be forgotten") to the extent that processing is necessary

a) for exercising the right of freedom of expression and information;
b) for reasons of public interest in the area of public health;
c) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes insofar as the exercise of the right to erasure would render impossible or seriously impair the achievement of the objectives of that processing;
d) for the establishment, exercise or defence of legal claims; or
e) for compliance with a legal obligation which requires processing 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.

2.5. RIGHT TO DATA PORTABILITY

If processing is necessary for performing a contract, or is based on your freely given consent and is carried out by automated means, You shall be entitled to obtain the data provided by You to the Controller in a machine-readable format. You shall have the right to have the personal data transmitted to another controller, where technically feasible. This right shall only apply to personal data disclosed by You; no other data may be transmitted (e.g. statistics, etc.).

You are allowed to:

- receive the personal data concerning You and available in the Controller's system in a structured, commonly used, machine-readable format,
- to transfer such data to another controller,
- to have the data transmitted directly to another controller, where technically feasible in the Controller's system.

That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.
The Controller fulfils the request for data portability exclusively upon a written request submitted via email or by post. In order to fulfil the request, it is necessary for the Controller to confirm that actually the person entitled to the right wishes to exercise such right. Within the framework of your right to data portability, You may request portability in relation to the data You provided to the Controller. Exercising the right shall not automatically result in the erasure of the data from the Controller's systems; therefore, You will continue to be registered in the Controller's system even after exercising such right, unless You request the erasure of your data.

2.6. OBJECTION TO THE PROCESSING OF PERSONAL DATA

On grounds relating to your particular situation, You may object to the processing of your personal data by way of a declaration submitted to the Controller if the legal basis for processing is

- public interest as per point (e) of Article (6)1 of the Regulation, or
- legitimate interest as per point (f) of Article (6)1 of the Regulation.

Where personal data are processed for direct marketing purposes, You shall have the right to object at any time to processing of personal data concerning You for such marketing, which includes profiling to the extent that it is related to such direct marketing. In such cases the personal data shall no longer be processed for such purposes.

If the right to object is exercised, the Controller shall no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims. In relation to establishing whether processing is justified by compelling legitimate grounds, the Controller shall make a decision. It shall inform you of its viewpoint in relation thereto in a written opinion.

You shall be entitled to object to processing in writing (via email or by post).

2.7. THE ENFORCEMENT OF RIGHTS OF A DECEASED DATA SUBJECT BY ANOTHER PERSON

Within five years following the death of the data subject, the person authorised by the deceased person to act or by means of a declaration recorded in an authentic instrument or a private document of full probative value shall be entitled to enforce the rights the deceased person was entitled to enjoy during his or her lifetime, such as the right of access, the right to rectification, erasure, restriction of processing, data portability and to object. If the deceased person made several declarations at the Controller, the person indicated in the declaration made at the later date may enforce such rights.

If the deceased person failed to make such a declaration, the rights the deceased person was entitled to enjoy during his or her lifetime and specified in the previous paragraph may be enforced by the data subject's close relative as per the Civil Code of Hungary within five years following the death of the data subject (if there are several close relatives, the close relative first exercising that right shall be entitled to enforce such rights).

According to point (1) of Section 8:1(1) of the Civil Code of Hungary, the close relative shall mean spouses, direct ascendants, adopted children, stepchildren and foster children, adoptive parents, stepparents, foster parents, brothers and sisters. The close relative of the deceased person shall certify the following:

- the fact and date of the death of the deceased data subject with a death certificate or a court decision, and
- his or her own identity – and if necessary, his or her close relative capacity – with an authentic instrument.

During the enforcement of the rights, in particular during proceedings vis-á-vis the Controller or before the National Authority for Data Protection and Freedom of Information and the court, the person enforcing the deceased person's rights shall have the rights and obligations the deceased person was entitled to and subject to during his or her lifetime pursuant to the Act on Informational Self-Determination and Freedom of Information and the Regulation.

Upon written request, the Controller shall inform the close relative of the measures taken, unless explicitly prohibited by the deceased person in his or her declaration.

2.8. DEADLINE FOR FULFILLING THE REQUEST

The Controller shall provide information on action taken to You without undue delay and in any event within one month of receipt of the request as per Sections 2.1-2.6. That period may be extended by two further months where necessary, taking into account the complexity and the number of the requests, but in such a case, the Controller shall inform You of any such extension within one month following the receipt of the request, together with the reasons for the delay, and of the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Where requests from You are manifestly unfounded or excessive, in particular because of their repetitive character, for the fulfilment of the request the 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 refuse to act on your request. The Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Where You make the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by You.

2.9. COMPENSATION AND TORT

Any person who has suffered material or non-material damage as a result of an infringement of the Regulation shall have the right to receive compensation from the Controller and/or processor for the damage suffered. The processor shall be liable for the damage caused by processing only where it has not complied with obligations of the Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Controller. The Controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

2.10. POSSIBILITIES TO ENFORCE RIGHTS

You may exercise your rights in a written request sent via email or by post.

You cannot enforce your rights if the Controller demonstrates that it is not in a position to identify You. Where requests from You are manifestly unfounded or excessive, in particular because of their repetitive character, the Controller may charge a reasonable fee for the fulfilment of the request or refuse to act on the request.
The Controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. Where the Controller has doubts concerning the identity of the natural person making the request, the Controller may request the provision of additional information necessary to confirm the identity of the person making the request.

Based on the Act on Informational Self-Determination and Freedom of Information, the Regulation and the Civil Code of Hungary (Act V of 2013), You

a. may lodge a complaint with or submit a request to the National Authority for Data Protection and Freedom of Information (H-1055 Budapest, Falk Miksa utca 9-11; https://www.naih.hu),
   OR
b. may enforce your rights before the court. An action may be brought, at your choice, before the regional court based on your place of residence (the list and contact details of regional courts are available via the following link: https://birosag.hu/torvenyszekek).

3. MANAGEMENT OF PERSONAL DATA BREACHES

Personal data breach means 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. The Controller shall keep a record for the purpose of checking the measures related to personal data breaches, providing information to the supervisory authority and You; the record shall include the personal data concerned, the data subjects and their number, the date and time, the circumstances and the effects of the breach as well as the measures taken to eliminate such breach. In the case of a personal data breach, the Controller shall, without undue delay but not later than 72 hours, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to your rights and freedoms, the Controller shall communicate the personal data breach to You without undue delay.

4. ACCESS TO DATA AND DATA SECURITY MEASURES, DATA TRANSFER

4.1. ACCESS TO DATA, DATA TRANSFER

The personal data are accessible to a strictly limited number of the Controller's employees and particular agents for the purpose of performing their tasks.

The Controller shall only provide the personal data processed by it to other bodies and public bodies (recipients) in ways and for the purposes specified by law.

The Controller informs You that the court, the prosecutor, the investigation authority, the authority dealing with administrative offences, the administrative authority, the National Authority for Data Protection and Freedom of Information, or in accordance with statutory authorisation, other bodies may request the Controller to provide information, disclose or hand over data, or make documents available.

The Controller shall disclose personal data to the authorities, if the authority indicated the exact purpose and the set of data, in the quantity and to the extent absolutely essential to achieve the purpose of the request.

4.2. DATA SECURITY MEASURES

The Controller shall take every reasonable measure to ensure data security and provide an appropriate level of protection in particular against unauthorised access, alteration, transfer, disclosure, erasure or destruction as well as accidental destruction and corruption. The Controller shall ensure data security by applying appropriate technical and organisational measures.

The Controller shall choose and operate the IT devices applied for the processing of personal data during the provision of the service in a manner that:

- the processed data are available to the authorised persons (availability);
- the authenticity and authentication of the processed data are ensured (authenticity of processing);
- the unaltered state of the processed data is verifiable (data integrity);
- the processed data are protected against unauthorised access (data confidentiality).

During processing the Controller shall maintain

- confidentiality: it shall protect the information so that only the authorised persons may have access thereto;
- integrity: it shall protect the accuracy and completeness of the information and the processing method;
- availability: it shall ensure that when it is necessary for the authorised user, the desired information is actually accessible and the related tools are available.

In order to ensure compliance with the above requirements, the Controller shall, from time to time, make backups of the data available in its system, including your personal data. The legal basis for this processing activity is the Controller's legitimate interest, i.e. data recovery in the case of any data loss. Additional details are available in the Controller's Regulation on backup. Further information may be requested via the adatvedelmitisztviselo@keler.hu email address.

The protection of personal data is further ensured by the fact that the Controller engages a data protection officer who is accountable to the Controller's senior management and shall not act under the instruction of any person when performing his or her tasks.

Where processing is to be carried out on behalf of the Controller, the Controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the requirements of the Regulation will be met and the protection of your rights will be ensured.

5. MISCELLANEOUS PROVISIONS

The Controller reserves the right to unilaterally modify this Privacy Notice. If any change is made regarding the content of the Privacy Notice, the Controller shall notify You thereof by disclosing the modification on the Controller's website and indicating the date of entry into force of the new Privacy Notice.

If you provided the data of another natural person or fictitious data to the Controller and caused any damage thereby, the Controller shall be entitled to enforce its claim for compensation against You.

The Controller does not check the personal data provided to it. Exclusively the person providing the data shall be responsible for the accuracy thereof. Upon the provision of your personal data, You assume responsibility for the fact that the provided data are true and that those are your own personal data.