INFORMATION NOTICE
ON THE PROCESSING OF PERSONAL DATA
Edition 03.07.2024

UNICREDIT BANK SA, a company managed in a dualist system, registered with the Trade Register under the number J40/7706/1991, sole registration code 361536, fiscal attribute RO, headquartered in Bucharest, 1F Expozitiei Bvd, 1st sector, subscribed share capital and paid RON 455.219.478,30, enrolled within the Banking Registry under the number RB- PJR-40-011/18.02.1999 , hereinafter referred to as the "**Data Controller**" or the "**Company**" processes your personal data as a Data Subject, hereinafter referred to as the "**Data Subject**", in good faith and in accordance with the provisions of Regulation (EU) no. 679 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 (UE Regulation hereinafter referred to as the **"GDPR"** and in achieving the purposes specified in this Information Notice.

1. The Data Controller:

The Data Controller, as identified below, is a Romanian company established and operating according to the laws of Romania, which, in its capacity as employer/beneficiary of the services provided, stores in good faith the personal data of its employees/collaborators and of the candidates for the vacancies offered by it, in accordance with the labor legislation and other applicable regulations, fully respecting the principles of data processing of personal data for legitimate purposes, in accordance with the applicable legal provisions.

2. Personal Data

In your capacity as a candidate or Data Subject for a position within the Company, the Company expressly informs you, through this Information Notice, in accordance with Articles 12 and 13 of the GDPR regarding the processing and storage of your personal data, under the conditions described in this Information Notice:

2.1. Proof of identity and eligibility for employment such as: name, surname, date of birth, home address, marital status, telephone number and email address, nationality, citizenship, gender, facial image – photo (if available in the resume), personal identification number (hereanafter called **PIN**), hobby data, personality data, video image and voice of the Data Subject (available through remote communication means), the content of the remote interview, the environment of the location where the Data Subject is located, the date and duration of the interview (when the unrecorded interview is conducted through remote communication means such as Microsoft Teams/www.microsoft.com platforms), other data from the resume/identity card/passport, data regarding professional experience, studies, professional certificates or certificates issued by the regulatory authorities, professional skills and competencies and other similar categories of data;
2.2. Pre-employment checks such as: references, interview notes, records/results of pre-employment checks, including checks on the criminal/tax record (only when there is a legal obligation to do so), disciplinary sanctions, information included in the Data Subject's resume and/or in any application forms, other similar categories of data. For personnel occupying managerial/management/coordination positions that involve the processing of a significant volume of data and the management of the associated risks, the integrity and good reputation are verified by signing a declaration containing information on some crimes related to the exercise of the duties of service. The signing of this declaration also takes place in the context of prudential management of the Company's reputational risk and the reduction of the possibility of subsequent occurrence of risks of any nature (such as operational, judicial, compliance) that may prejudice the Company. After the date of employment/beginning of the collaboration relationship, no decisions will be made regarding the Data Subject in relation to that statement.
2.3. The employment conditions such as: records regarding the job offer and its acceptance, professional experience, the employment contract belonging to the Data Subject, the agreed work schedule, the duration of the probation period, the duties related to the position, the modification of the job description and the reason for the change, as well as the s relation of subordination, the address of the job, the position, the occupation, the data regarding the relocation, if applicable, details regarding the hierarchical superior and the person responsible for the employment, details regarding training courses, individual training programs, other similar categories of data;
2.4. Data regarding external income and activities such as: field of activity, time allocated (hours/day, days/week), whether or not the activity is remunerated, the level of remuneration (expressed as a percentage, compared to the salary in the Company), membership in the management of an entity outside the UniCredit Group (as identified on the UniCredit Group website at: http://www.unicreditgroup.eu/dazen "Selected financial and lending institutions of the UniCredit Group") and the status of associate/shareholder of a company (name of entity and position), membership of a committee or commission within a regulator/supervisory authority, a ministry, an organization, other similar categories of data;
2.5. Data regarding relatives/relatives such as: name, surname and degree of kinship of relatives/relatives employed in the UniCredit Group, other similar categories of data;
2.6. Technical/information and communication technology data: Logs related to interviews that take place through remote communication means such as Microsoft Teams, the provider being an independent data controller. These logs may be processed by the Company to the extent that they are stored by the Company's technical means or become accessible to it; such logs may concern information such as the date and duration of the interview conducted by means of remote

communication, email addresses or phone numbers involved in this activity. For the avoidance of any doubt, the Data Subject is encouraged to go through the information related to the protection of the personal data available on the website of the application provider, the section dedicated to the protection of personal data. In cases where the Company would use means of remote communication other than Microsoft Teams, the Data Subject may collect information about the protection of the personal data by previously visiting the website belonging to the application provider (independent data controller), considering the name of this provider that may be comprised by the link for interview sent to the Data Subject by the Company; also, the Data Subject is encouraged to periodically visit afterwards the website belonging to the application provider, data protection section;
2.7. **If the Data Subject receives a employment/collaboration offer from the Company, for the duly conclusion of the employment/collaboration relationship, data related to the compliance analyses on the Data Subjects are previously processed for the proper management of the significant risks, in particular the reputational risk, in areas such as checks of the integrity/reputation of the Data Subject, aspects that also include areas such as the verification of conflicts of interest, prevention of money laundering and terrorism financing, international sanctions.**
In this context, the Company processes, including from commonly used public sources, data such as: (i) information regarding accusations, investigations, onvictions and measures related to crimes such as money laundering, terrorist financing, fraud, the entity handling the file, the status of the file, the solutions pronounced and the like, political exposure, important public office held, status as a publicly exposed person, the capacity of beneficial owner and the like, according to the applicable legislation and regulations; (ii) international sanctions, the content of such measures, the duration, the entity that has instituted/monitors such a measure, information on the assets subject to sanctions, bank information such as a measure of unavailability of accounts, as a result of a sanction and the like, according to the applicable legislation and regulations.
2.8. Any other similar categories of data derived from law enforcement, signed documentation, other related processing, regardless of the basis for processing.

3. Purpose of personal data processing:

3.1. Your personal data are processed by the Company for the purpose of carrying out recruitment activities on the basis of a contract that can be concluded in the future upon the request of the Data Subject, which also implies the previous preparation of the employment offer/other related documents, in case you are eligible, based on the provisions of the Article 6, 1st paragraph, letter b) from the GDPR;
3.2. In the event that the recruitment process ends with the submission of an employment/collaboration offer to you, your personal data will be processed by the Company for the conclusion of the employment/collaboration contractual relationship, by prior compliance analyzes for appropriate management of significant risks, especially reputational risk, in areas such as checking the integrity and reputation of the Data Subject, aspects that also include areas such as conflict of interest, prevention of money laundering and terrorist financing, international sanctions, based on the legitimate interest of the Data Controller to take all the necessary measures for the prudential management of the significant risks (especially reputational risk), according to the Article 6, 1st paragraph, letter f) from the GDPR and of the Company's legal obligation to establish appropriate standards regarding the integrity, experience and training of the involved personnel, according to the relevant legislation (such as in BNR Regulation no. 5/2013) and of the Article 6, 1st paragraph, letter c) from the GDPR;
3.3. Reducing the risk of litigation, claims/requests of any type, complaints, coming from any natural or legal person, such as Courts of law, supervisory authorities, auditors, by the Company taking the necessary and useful measures to support the defense of rights and interests in accordance with the relevant legislation, according to the Article 6, 1st paragraph, letter f) from the GDPR.

4. Duration of data processing:

4.1 If you will be employed, your data, including your resume, will be stored in the personnel file, according to the legal provisions in force, namely 75 years from the termination of the contractual relationship, taking into account the provisions of the Law no. 16/1996 on the National Archive;
4.2. In the situation in which you will not be employed: (i) your resume will be retained for a maximum period of 3 years, based on the legitimate interest of the Company to ensure the human resources necessary for the optimal performance of its current activity, in accordance with the applicable legislation. If you do not wish to be contacted by the Company in the future for various vacant positions, appropriate to your professional profile, you can object to such processing, according to the Article 6 below; (ii) the data mentioned by the Articles 2.1., 2.2, 2.3. 2.4., 2.5, 2.7. are stored 30 days after the decision regarding the selection of the candidate for the open position;
4.3. The logs mentioned by the Article 2.6 (derived from processes such as remote recruitment), are kept 10 years after their creation;
4.4. Personal data regarding video surveillance to ensure the security of goods and persons will be stored for a period of max. 30 calendar days, respectively in accordance with the grounds provided by the legislation in force, with the exception of cases when there is a legitimate interest of the Company, when they are stored until the date of realization of the pursued legitimate interest;
4.5. The data will be stored in a safe place and in accordance with the conditions and legal provisions.

5. Data processors/Recipients/Joint-Controllers/Independent Data Controllers:

Your personal data may be processed, in full compliance with the legislation on the protection of personal data, by:

5.1 Providers of recruitment services, providers of remote communication means for recruiting (independent data controllers), providers of labor services or human resources consulting services. Providers of IT services and systems, such as Total Soft SA or archive, as well as all the companies in these categories of recipients from whom the Data Controller will contract services and products and which have taken adequate protection measures, according to the legal provisions, in order to ensure that they comply with their obligations regarding the protection of personal data. If the data processors subcontract part of the activities involving the processing of personal data, the subcontractors will be subject to the same obligations regarding the implementation of the security, technical and organizational measures provided by the applicable legislation.
5.2 State authorities such as Territorial Labor Directorate, tax authority, consulates or embassies for issuing visas, etc. based on their powers provided by the applicable law;
5.3 UniCredit Group companies that provide activities for the Company in the field of labor relations or to which the Company reports the results of its activity, including but not limited to the company that provides IT services (UniCredit S.p.A.)

6. The candidate's rights regarding his personal data:

We would also like to inform you that, according to the applicable legal provisions, including but not limited to Articles 12-22 of the GDPR, you have the following rights: **6.1.** the right to information and access to your personal data; **6.2**. the right to rectify your data; **6.3**. the right to be forgotten/the right to data deletion; **6.4**. the right to restrict processing; **6.5.** the right to data portability; **6.6**. the right to object to the processing of your data, in the case of personal data processed in accordance with Article 6, 1st paragraph, letter e) or f) from the GDPR, including the creation of profiles based on these provisions, respectively for the performance of a task performed in the interest publicly or within the exercise of an official authority with which the Company is vested, respectively for the purpose of the legitimate interests of the Company; **6.7.** the right not to be subject to an individual decision, which means that you have the right to request and obtain the withdrawal, cancellation and reconsideration of any decision that produces legal effects on you, adopted exclusively on the basis of a personal data processing operation by means automated, in order to evaluate some personality traits, such as professional skills, credibility, your behavior at work; **6.8.** the right to withdraw your consent at any time for processing based on consent, while maintaining the validity of the processing carried out until the date of withdrawal of consent; **6.9.** the right to notify the National Supervisory Authority for the Processing of Personal Data (**local Supervisory Authority/SA**) or any competent Courts of law.

To exercise these rights, you can contact the Company through a written, dated and signed request - to the attention of the Recruitment Team or by email to the address: jobs@unicredit.ro with the exception of the exercise of the rights provided for in point 6.9., which are exercised by a written request to the local SA or submitted by the competent Court of law. Your request will be analyzed and you will be answered within one month from the date of receipt of the request, with the possibility of extending the response period by two months, in case of complexity/significant volume of the requests, specifying that the Company will inform you in this regard within the initial one month term. In case of repeated requests, the Company may charge a fee. Contact details of the Data Protection Officer: dpo@unicredit.ro

6. International data transfer:

Personal data will be transferred (e.g. accessed, consulted, etc.) to other UniCredit Group companies in other countries, in order to initiate, conclude and develop contracts and/or projects with an entity from the Group or collaborators of the Company, such as, but without being limited to databases, respectively in third countries that ensure an adequate level of protection of personal data where the presence of the UniCredit Group is ensured, as identified on the website of the UniCredit Group at the address: http:// www.unicreditgroup.eu/dazen ("Selected financial and credit institutions of the UniCredit Group"). In all situations where the international transfer of data will be necessary, this will only be achieved if an adequate level of personal data protection recognized by decision of the European Commission, such as member countries of the European Economic Union (EEA). In the absence of such a decision of the European Commission, the Company will be able to transfer personal data to a third country only if the person who will process the data has provided adequate guarantees provided by law in order to protect personal data (such as standard contractual clauses) . The Company can be contacted to obtain additional information on the safeguards offered to protect personal data in the case of each data transfer abroad, through a written request in this regard.

7. Other aspects:

The Data Controller guarantees that it processes your data under legal conditions, while also implementing appropriate technical and organizational measures to ensure data integrity and confidentiality according to the Articles 25 and 32 of the GDPR. The answer regarding the result of the recruitment process is communicated to the Data Subject within the term and method communicated in the recruitment process. The Data Subject is informed of the fact that, if she/he finds out about a certain opening in the Company, through the facilitation of an employee/collaborator of the Company and applies for it, and if, during the recruitment and selection processes in the Company, including after he becomes an employee/collaborator of the Company, will communicate to the Company, upon request, the name of the person mentioned above and/or related

information (for reasons including the Company's encouragement and bonusing of such behaviors), undertakes to communicate this document to that person by any mean of communication (such as email, sms with an attached document) within a maximum of one month from the communication of the data regarding that person to the Company and to remit this proof to the Company, upon request.

UNICREDIT BANK SA

Candidate
[Name & surname]

....

Signature

....

Date .....