Valid from: 27/08/2024

THE NOTICE OF PAYSERA LT, UAB ON CANDIDATES' PERSONAL DATA PROCESSING

CHAPTER I

GENERAL PROVISIONS

1. Following the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and other legislation regulating the protection of personal data, this Privacy Notice to Candidates (hereinafter referred to as the Notice) establishes the procedure according to which the Company processes the personal data of an individual client participating in the selection for the vacant position.

2. The provisions of the Notice shall apply to an individual client participating in the selection for the vacant position at Paysera LT, UAB.

CHAPTER II

TERMINOLOGY

3. Terminology and abbreviations used in this Privacy Notice to Candidates have the following meanings:

3.1. Personal data shall mean any information related to an individual client who can be identified directly or indirectly (e.g. name, surname, contact details, etc.).

3.2. Person shall mean an individual client (data subject) the data of whom is being processed.

3.3. GDPR shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3.4. Data processing shall mean any operation which is performed on the personal data of the person (e.g. collection, recording, storage, giving access, transferring, etc.).

3.5. Company shall mean Paysera LT, UAB (data controller) conducting the selection for the vacant position the Candidate applied to, as well as its partners in other countries.

3.6. Candidate shall mean a person applying for a vacant position (job).

3.7. Other terminology used in the Privacy Notice shall be understood as it is described in the legislation regulating the protection of personal data (GDPR, Law of the Republic of Lithuania on Legal Protection of Personal Data, and others).

CHAPTER III

OBJECTIVES AND LEGAL GROUNDS OF PERSONAL DATA PROCESSING

4. The Company shall process the personal data only for particular purposes and on the grounds laid down in the legislation when:

4.1. The processing is necessary for the purposes of recruitment, preparation, conclusion and/or performance of an agreement concluded with the data subject;

4.2. The data subject has given consent to process their data for one or several specific purposes by submitting a CV or in any other way;

4.3. The Company must process personal data in compliance with legal requirements;

4.4. Personal data must be processed pursuant to the legitimate interests of the Company.

5. The main objectives pursued by the Company while processing personal data are the following:

5.1. Conducting employee selections. The Company shall process personal data on the grounds of consent when a person submits their CV or other information as they participate in selections for the positions announced by the Company, or as they wish to carry out their internship.

5.2. Concluding and performing employment agreements. The Company shall process personal data when concluding and on the basis of intention to conclude an employment agreement or perform the employment agreement concluded with a candidate;

5.3. A criminal record check of the candidate is carried out before a person is employed in a particular position according to the Company's internal regulations. The Company shall process personal data when verifying impeccable reputation based on legitimate interests or legislation requirements.

5.4. Responding to submitted questions. The Company shall process personal data when examining and responding to submitted questions and claims on the grounds of the agreement, consent, or legislation requirements.

5.5. In any case, the Company organising the selection for a specific vacant position shall be considered the data controller of the Candidate's data, while a third party (if any) performing the selection or part of it – the data processor.

6. In all cases mentioned above, the Company shall process personal data in compliance with data protection requirements only to the extent necessary to meet clearly defined and legitimate purposes.

CHAPTER IV

PERSONAL DATA PROCESSING CATEGORIES

7. The main categories of personal data processed by the Company for the aforementioned purposes and legal bases are the following:

7.1. Identification data – name, surname, date of birth, etc.;

7.2. Contact details – address, phone number, email, etc.;

7.3. Professional data – education, qualifications, professional skills, business qualities, etc.;

7.4. Data on impeccable reputation – data related to criminal record (for a limited number of positions);

7.5. Other information voluntarily submitted by the candidate participating in the selection.

8. The Company shall process personal data in accordance with the legal grounds specified in this Notice, the Privacy Policy and legislation.

CHAPTER V

CANDIDATE DATA PROCESSING FOR PERSONNEL SELECTION PURPOSES

9. The Company shall process candidates’ personal data in order to evaluate if the person is eligible to hold office or perform job functions. The data of persons submitting their candidacies to participate in one or several ongoing selections – i.e. all vacant positions for which the person has applied are visible to the persons conducting the selections. This data will be processed (visible in Paysera LT, UAB HR management system) for as long as other candidates' personal data is processed, depending on the consent provided or until the person revokes consent for data processing.

10. Personal data submitted by the person to the Company by sending their CV, cover letter and other information seeking to participate in selections for vacant positions or internships are stored and used within the scope and for the purposes of those selections.

11. Subject to the employee's consent, personal data shall be stored and used for 2 (two) years after the evaluation of the person’s candidacy (both successful and unsuccessful), until the person makes a voluntary decision not to participate in the selection or revokes their consent to process such data. The term for storing personal data shall be calculated from the evaluation of the last candidacy a person participated in.

12. A person who expressed their willingness to participate in the selection for a vacant position or an internship shall be responsible for transferring their data to the Company and shall have an unrestricted right to manage this data, i.e. in the account created in the Candidate Portal system the candidate may at any time:

12.1. Consent/revoke the consent to use their personal data in the selection procedures conducted by the Company when applying for a specific vacant position;

12.2. Request rectification of inaccurate information about themselves, exercise the right to be forgotten;

12.3. Access the information collected in the Company about them for selection purposes;

13. It should be noted that in order to participate in the selections announced by the Company, a person must agree to the processing of their data as a candidate by indicating that they have read and understood the Company’s Privacy Notice to Candidates.

14. A person who did not give consent to use their personal data in other selections when submitting their candidacy will be asked to give their consent. The candidate must provide consent to use their personal data in selections conducted by the Company within 30 (thirty) calendar days from the date the Notice was sent to them.

15. The reminder to provide consent for the use of personal data in ongoing selections may be sent twice – upon receipt of the candidacy and after the selection ends.

16. It should be noted that if the candidate does not provide any response within 30 (thirty) calendar days from sending the second notice, their data will be deleted from the database of selections conducted by the Company.

17. The Company has a recommendation system where employees of the Company can provide information on potential candidates. The employee who recommends a candidate undertakes to inform the potential candidate about the provision of their personal data to the Company. After a potential candidate has been recommended, they shall receive an automated email containing the request to use their personal data in the selections conducted by the Company.

18. The Company follows the principles of transparency, impartiality, and zero tolerance to corruption, therefore one of the requirements for candidates is an impeccable reputation. For this purpose, the Company collects publicly available personal data related to the impeccable reputation of the candidate who is eligible to hold office or carry out job functions. We ask candidates who are offered to conclude an employment agreement to provide the following personal data for verification: name, surname, and date of birth when personal data is collected on the basis of legitimate interest. For candidates offered to conclude an employment agreement for positions with a high risk of corruption or strategic positions, the Company processes personal data in the scope and on the basis of legislation requirements. Personal data of candidates for verification of impeccable reputation shall be stored for 10 years after termination of the employment agreement. We will conclude an employment agreement with the candidate only after we receive a positive conclusion on the impeccable reputation of the candidate.

19. For the purposes of personnel selection, the Company may collect the candidate's personal data related to qualification, professional skills and business qualities from the previous employer by informing the candidate thereof, and from the current employer – only upon receiving the consent of the candidate.

CHAPTER VI

CANDIDATE DATA PROCESSING FOR THE PURPOSE OF IMPROVING THE SELECTION PROCESS QUALITY

20. In order to improve the quality of the selection process, the Company shall ask the candidate for feedback on the experience of participating in the selection process by sending a survey to the email provided by the candidate.

21. Candidate personal data for the purpose of carrying out the survey shall be processed based on provided consent. Candidate data shall be processed for 2 (two) years after consent has been given, or until the candidate revokes their consent to processing such data. Candidates shall have the right to revoke their consent at any time without providing a motive by clicking “Unsubscribe”. Revocation of consent shall not affect the lawfulness of processing based on consent carried out prior to revocation of consent.

CHAPTER VII

CANDIDATE DATA PROCESSING FOR THE PURPOSE OF SENDING NOTIFICATIONS ABOUT VACANT POSITIONS

22. Candidate personal data for the purpose of sending notifications about vacant positions shall be processed based on the provided consent. Candidates shall have the right to revoke their consent at any time without providing a motive. Revocation of consent shall not affect the lawfulness of processing based on consent carried out prior to revocation of consent.

CHAPTER VIII

OBTAINING PERSONAL DATA

23. The Company shall process personal data provided by data subjects themselves or obtained from other sources, such as:

23.1. After employees of the Company recommend the Candidate;

23.2. From social networks for professionals (e.g. LinkedIn, etc.);

23.3. State, law enforcement authorities (only for positions with a high-level risk of corruption or strategic positions);

23.4. Third parties (e.g. current and/or previous employer of the candidate), etc.

24. In all cases mentioned above, the Company shall process personal data only to the extent necessary based on an agreement, consent, legislation, or the legitimate interest of the Company.

CHAPTER IX

PROVIDING PERSONAL DATA

25. Following legal requirements, the Company may transfer processed personal data to the recipients of the data under the following categories:

25.1 Service providers. The Company may transfer the processed personal data to third parties operating on behalf of the Company and/or under its instructions that provide the Company software licensing, maintenance, employment relationship administration, accounting, correspondence and other services in order to ensure proper provision, management and development of the Company’s services. In such cases, the Company shall take appropriate measures to ensure that the service providers (data controllers) involved process the personal data provided only for the purposes for which they were provided by ensuring appropriate technical and organisational security measures, compliance with Company instructions and applicable legal requirements;

25.2. Government, law enforcement, and supervisory authorities. The Company may provide processed personal data to government or law enforcement authorities (e.g. the police, the prosecutor's office, the Financial Crime Investigation Service, etc.) where it is mandatory under applicable laws or to protect the legitimate interests of the Company, employees or third parties;

25.3. Other third parties. The Company may provide personal data to other data recipients following legitimate grounds specified in the legislation.

CHAPTER X

APPLIED SECURITY MEASURES

26. The Company shall ensure the confidentiality of personal data in accordance with applicable legal requirements and the implementation of appropriate technical and organisational measures to protect personal data against unauthorised access, disclosure, accidental loss, alteration, destruction, or other illegal processing.

CHAPTER XI

AUTOMATED DECISION-MAKING AND PROFILING

27. The Company does not process candidates' personal data by means of automated individual decision-making and profiling as provided for in Article 22 of the Regulation.

CHAPTER XII

RIGHTS OF DATA SUBJECTS

28. After contacting the Company and confirming their identity, the person has the right to:

28.1. Access personal data processed by the Company regarding themselves;

28.2. Request to rectify incorrect, incomplete, inaccurate personal data regarding themselves;

28.3. Request to erase personal data or suspend, except for storing, data processing actions if it infringes the requirements of the applicable legislation or if personal data is no longer necessary to achieve the purposes for which it was collected or otherwise processed;

28.4. Receive personal data provided by themselves in a structured, commonly used, and machine-readable format;

28.5. Restrict the processing of their personal data in accordance with the applicable legislation, e.g., for the period during which the Company will evaluate whether the person has the right to request erasure of their personal data;

28.6. Object to the processing of their personal data and/or in case personal data is processed based on consent – revoke the given consent for processing their personal data at any time without prejudice to the lawfulness of processing based on consent prior to revocation. In case consent for personal data processing is revoked before the end of the selection, the person simultaneously revokes further participation in that selection.

29. You can contact us regarding this Privacy Notice to Candidates or the processing of personal data conducted by the Company in writing at Pilaitės pr. 16 Vilnius or by email dpo@paysera.com

30. Should the issues related to the processing of your personal data conducted by the Company and/or your rights are not resolved, you also have the right to submit a claim to the supervisory institution – the State Data Protection Inspectorate, ada@ada.lt.

CHAPTER XIII

VALIDITY AND AMENDMENTS OF THE PRIVACY NOTICE TO CANDIDATES

31. Additional information on how the Company processes personal data may be provided on the website paysera.lt or by other means (e.g. by email, etc.).

32. The Company shall have the right to unilaterally amend/supplement this Privacy Notice to Candidates. The Company shall inform about the amendments to the Privacy Notice to Candidates by publishing it on the website paysera.lt. In certain cases, the Company may also inform data subjects about the amendments in the candidate selection systems or by other means (e.g. by email, etc.).

CHAPTER XIV

FINAL PROVISIONS

33. The supervision and control of the requirements provided in the Privacy Notice to Candidates shall be ensured by employees carrying out the compliance functions within the Company.

34. The Privacy Notice to Candidates and amendments thereof shall be coordinated with the Data Protection Officer of Paysera LT, UAB.

Annexe No.1 to the Notice of Paysera LT, UAB on Candidates' Personal Data Processing

LIST OF POSITIONS SUBJECT TO THE REQUIREMENT OF IMPECCABLE REPUTATION

Following the Law of the Republic of Lithuania on Electronic Money and Electronic Money Institutions, the Law on Banks, the Law on Legal Protection of Personal Data, GDPR provisions, and in order to ensure an impeccable reputation and operational transparency, Paysera LT, UAB collects criminal record data of employees in the following positions:

1. **Top-level managers** – because the collection of data on these individuals is mandated by legal acts. Moreover, managers make strategic decisions that can significantly affect the Company's operations and financial position, so it is important to ensure that they are reliable and have not committed serious financial or economic crimes in the past.
2. **Employees performing client due diligence functions** – because these employees have access to confidential client data, the protection of which is extremely important for client interests. By checking their criminal records, the probability of data being used illegally can be reduced, thus protecting clients' identities and financial information.
3. **Employees performing anti-money laundering functions** – because these employees are responsible for combating money laundering, which is important for the security of society and the state. By ensuring that they have not been convicted of related crimes, society can be better protected from financial crimes and their consequences.
4. **Employees executing payment transactions** – because these employees receive and issue large sums of cash, so checking criminal records can help ensure that employees have not been convicted of financial crimes, thus protecting clients' assets.
5. **Employees performing financial operations** – because these employees manage the Company's financial operations, so the legality of their actions directly affects the interests of clients and society.
6. **Client support specialists** – because they have access to clients' personal and financial data, which they could potentially misuse.

Data on candidates' impeccable reputation is collected if the candidate is selected for the position. Failure to provide this information is grounds for the employer to refuse to enter into an employment agreement.

Agreement History

THE NOTICE OF PAYSERA LT, UAB ON CANDIDATES’ PERSONAL DATA PROCESSING (valid until 2024.08.27)