PROCEDURE FOR THE PROCESSING OF CANDIDATES PERSONAL DATA

1.General provisions
1.1. Information on the data controller and the contact details of the Data Protection Officer Data controller: Maneuver LT, UAB Registration code: 304785124 Head office address: Žalgirio st. 92-510, LT-09303, Vilnius, Lithuania Phone: +370 5 214 1409 Email: info@genome.eu **Contact details of the Data Protection Officer**: E-mail: dpo@genome.eu
1.2. This Procedure establish the conditions for the collection and processing of personal data of candidates for the job position in the UAB "Maneuver LT" (hereinafter - Company), which is executed by the Company as a data controller for the purposes of recruitment. During the recruitment process, the Company processes the personal data of the candidates in accordance with the procedure established in this Procedure and ensures the security of these data.
2.Purpose of data processing
2.1. Purpose of processing personal data of candidates: carrying out the recruitment of the Company's staff and assessing candidate suitability for the respective positions.
2.2. For the purpose mentioned in point 2.1. the Company collects, analyzes, stores and otherwise processes the personal data of the candidates in written (including electronic) form.
2.3. The purpose of the processing of candidates' personal data shall include:
2.3.1. Determining the candidate's qualifications, competencies, and assessing professional suitability;
2.3.2. Determining the candidate's professional (work) experience and assessing suitability;
2.3.3. Determining the candidate's personal and business qualities and assessing suitability;
2.3.4. Assessing the alignment of the candidate's and Company's values;
2.3.5. Assessing candidate suitability pursuant to requirements applicable to electronic money institutions supervised by the Bank of Lithuania, including fit and proper, impeccable reputation, and conflict of interest (COI) assessments;
2.3.6. Preparation and submission of an offer to conclude an employment contract to the candidate.
3. Basis of data processing
3.1. The legal basis for the processing of candidates' personal data for the specified purpose is the candidate's consent. The candidate has the right to withdraw their consent at any time, without any negative impact on their application. To withdraw consent or exercise any other rights set out in this Procedure, you may contact our Data Protection Officer at any time via email: dpo@genome.eu.
3.2. The Company's consent to process the data provided in the CV and / or other application documents (curriculum vitae, cover letter, etc.) for the purpose provided for in this Procedure shall be deemed received by the Company when the candidate submits his / her CV, candidate application form and / or other documents.
3.3. If the Company receives information about the candidate and / or CV and / or other application documents from employment services, employment agencies, job search online portals, career social networks (eg Linkedin) and / or other job search , selection and / or brokerage services, the Company assumes that the candidate has received all the necessary information about the processing of his / her data and has given his / her consent to the processing of his / her data to the relevant entity providing such services, which also includes the

right to provide your data to the Company, enabling the Company to process the candidate's data during the selection (s) for the job (s) and the evaluation of the candidate's candidacy.
3.4. The Company will collect the candidate's personal data from other sources only with the separate consent of the candidate. For example, the Company will only review the recommendations provided or seek feedback from another employer if the candidate agrees to contact the candidate's named employer and / or another person to receive feedback on the candidate.
3.6. Carrying out the recruitment of a head, a deputy or a member of the management body or a person responsible for the management of electronic money issuance activities, (Article 16 (2d) of the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania), Company must collect additional data (personal identification code, copy of passport) and personal data of special categories of candidates (eg on criminal record) with the consent of candidate (GDPR 6Art.1. a)) and also in order to fulfill the right obligation (GDPR 6str. 1d. c)) imposed on the Company (the candidature must meet the criteria set by the supervisory authority, information determined by the supervisory authority must be collected and the supervisory authority's approval must be obtained in accordance with E-money institutions Law Art. 16, BOL Resolution No. 03-181 On Approval of the Regulations on the Assessment of Managers and Key function holders of Financial Market Participants supervised by the Bank of Lithuania). However, the Company collects and processes such data only in case and to the extent necessary for the recruitment of a particular job position and to the extent permitted by applicable law.
3.6. If at the end of the recruitment for the respective job position the Company does not select a candidate and does not enter into a contract with him / her, the Company will destroy all personal data of the candidate collected for the purposes of the selection at the end of the selection, unless a separate consent has been obtained from the candidate for future recruitments (talent pool) under this Procedure.
4. Data sources
4.1. Usually, the Company receives the candidate's data directly from the candidate himself / herself - when the candidate responds to the Company's job advertisement and (or) submits his / her CV, candidate's questionnaire and / or other candidacy documents (CV, cover letter, etc.).
4.2. Information about the candidate, CV and / or other application documents may also be obtained by the Company from entities providing job search, selection and / or mediation services, e.g. from employment services, employment agencies, job search web portals, specialized career social networks (eg Linkedin), when the Candidate applies through the Company's "Career Site" by entering their Linkedin account link.
4.3. The Company may also obtain certain information about the candidate from third parties, e.g. referees, current or former employers. However, the Company will only collect such information if the candidate consents to the Company contacting the candidate's designated employer and / or other person to obtain a recommendation or feedback about the candidate. Certificates or extracts regarding criminal record / non-criminal record (which are mandatory for managerial positions under the supervisory requirements of the Bank of Lithuania) are obtained by the Company directly from the candidates or managers themselves, following a request by the Company to provide them in accordance with fit and proper and impeccable reputation assessment requirements established by the Bank of Lithuania.
5. Information on data transmission, recipients and processors
5.1. The data of the candidate for the new job shall be stored only by the person authorized by the Company, who is obliged to work with the recruitment data in his/her mail and / or computer, no more than to the end of the recruitment. Only a person authorized by the Company may access the candidate's data.
5.2. Categories of data recipients:
5.2.1. Personnel recruitment and (or) assessment service providers or consultants providing services related to selection, evaluation of candidates and internal administration;
5.2.2. Controlling company and its representatives (for certain important positions)
5.2.3. Supervisory authorities (if the selection is made for positions that are notifiable to the relevant supervisory authority);
5.2.4. State, law enforcement authorities or courts (in case of dispute).

5.3. Categories of data controllers: IT service providers, database software providers, database administration service providers, data center, hosting and cloud service providers.
5.4 Candidates' personal data shall not be transferred to third countries or international organizations.
5.5. In each case, the Company shall provide the data processor or recipient only with the amount of data necessary for the execution of a specific order or provision of a specific service. The data processors by the Company may process the personal data of the candidate only in accordance with the instructions of the Company and may not use them for other purposes or transfer them to other persons without the consent of the Company. In addition, they must ensure data security in accordance with applicable law and written agreements with the Company.
6. Personal data
6.1. Personal data means any information that can be used to identify a person, as well as any information about a person that has already been identified.
6.2. Personal data provided by candidates processed by the Company:
6.2.1. Name, surname;
6.2.2. telephone number; Email address;
6.2.3. Curriculum vitae (according to the form chosen by the candidate), data on qualifications, professional skills, education, professional (work) experience;
6.2.4. Information on language skills, information technology skills, other competencies;
6.2.5. Diplomas, certificates, training;
6.2.6. Written recommendations and data contained therein;
6.2.7. Other personal data provided by the candidate voluntarily (submission of data is not necessary, the candidate submits data voluntarily).
6.3. If a candidate is running for the position of manager, deputy manager, member of the management body or person responsible for the management of electronic money issuance activities (Article 16 (2d) of the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania), the following additional information shall be collected:
6.3.1. Data on the candidate's criminal record / non-criminal record *;
6.3.2. Data of impeccable reputation * and other information according to the questionnaire of a member of the management body and/or key function holder of the financial market participant supervised by the Bank of Lithuania;
6.3.3. Identity code;
6.3.4. Copy of identity document.
6.4. Conflict of Interest (Declaration of Conflicts / Interests) as a Candidate Suitability Requirement:
6.4.1. As an electronic money institution supervised by the Bank of Lithuania, the Company is subject to statutory requirements to ensure strict risk management, transparency, and comprehensive candidate suitability assessment. To comply with these requirements and the Company's Conflicts of Interest Management Policy, the Company carries out a conflict of interest assessment with selected candidates (finalists) before signing an employment contract, as an integral part of candidate suitability assessment.

6.4.2. For this purpose, selected candidates are requested to submit a completed Declaration of Interests form, which includes the processing of the following data:

- Direct or indirect holding of 10% or more of the share capital or voting rights in any company (legal entity name, code, activity, portion of shares/voting rights);
- Significant influence over other legal entities by means other than shareholding (directorship, board or committee member, procurist, etc.);
- Existing or intended contracts (employment, service agreements, orders, consultancy, external assignments, or other professional activities) not related to the Company while working at the Company;
- Related persons (close relatives, family members) within the Company;
- Other circumstances or situations that could give rise to an actual or potential Conflict of Interest or influence objectivity and independence in performing duties at the Company.

6.5. In cases where there are reasonable doubts about the candidate's suitability for a specific position, before extending a formal job offer, the Company may initiate an additional job interview. During this interview, the candidate may be asked to provide the following personal data: date of birth, values, information on existing political relationships, and links with other organizations and/or states. In other words, if the company has reasonable doubts, it can conduct an additional information security check.

6.6. Automated decision making is not used for data processing.

** The Company collects and processes the personal data of special categories of candidates only if and to the extent necessary for the selection for a specific job position and to the extent permitted by applicable law.*

7. Data processing deadlines

7.1. The Company shall process (store) the personal data of the candidates until the earliest of the following events:

7.1.1. An employment contract is concluded with the candidate;

7.1.2. The end of the recruitment to the job;

7.1.3. The candidate revokes the consent to process his / her personal data.

7.2. The Company may process the candidate's data for a longer period if the candidate has provided separate consent to process their personal data in order to assess suitability for future selections. In this case, upon obtaining separate consent, candidate data is retained for 2 (two) years following the final evaluation of the most recent candidacy, or until consent is withdrawn, whichever occurs earlier. Upon expiry of 2 years or withdrawal of consent, the candidate's data is immediately destroyed.

7.3. In other cases, the storage of personal data longer than specified in this Procedure may be carried out only when:

7.3.1. There are reasonable suspicions regarding an illegal act for which an investigation is being conducted;

7.3.2. The data of the candidate are necessary for the proper resolution of the dispute or complaint;

7.3.3. In case of other grounds provided for in legal acts.

8. Data protection

8.1. The Company shall protect the personal data of the candidates, ensuring their confidentiality, integrity and limited availability. Confidentiality means that the personal data of candidates are not disclosed to persons who do not have access to this data. Integrity means that candidates' personal data should be accurate, relevant and relevant to the purpose for which they are processed. Limited access means that only authorized persons have access to and process the personal data of candidates for legitimate and defined purposes.

8.2. The Company shall take the necessary technical and organizational measures to protect the personal data of

the candidates from unlawful processing and / or loss. The company installs the appropriate hardware and software, applies the necessary security measures (including physical and electronic access control).
9. Rights of data subjects
9.1. The data subject has the following rights enshrined in the GDPR:
9.1.1. the right to be informed of the processing of their data;
9.1.2. the right of access to the data;
9.1.3. the right to have the data rectified;
9.1.4. the right to have data erased ("right to be forgotten");
9.1.5. the right to restrict the processing;
9.1.6. the right to transfer data;
9.1.7. the right to object to the processing.
9.2. In order to protect the data of all its candidates from illegal disclosure, the Company, upon receipt of a person's request to provide data or exercise other rights, will request the submission of an identity document. Upon receipt of the Company's request for the exercise of any personal right and having ascertained the identity of the person, the Company undertakes to provide the person with information on the actions taken in response to the request without undue delay, but in any case, no later than one month after receipt of the request. If the Company refuses to comply with the request, it will do so with a reasoned response, substantiating it in the circumstances specified in the legal acts and informing the person thereof in writing.
9.3. Candidates' requests regarding his / her personal data shall be submitted to the Company's Data Protection Officer by email: dpo@genome.eu and examined in accordance with the procedure provided for in the Company's internal documents.
9.4. A candidate who believes that his / her rights related to the processing of his / her personal data by the Company have been violated has the right to apply to the supervisory authority: State Data Protection Inspectorate, Company code 188607912, L. Sapiegos g. 17, 10312, Vilnius, Tel. (8 5) 271 2804, 279 1445, El. E-mail ada@ada.lt, ways of submitting a complaint: https://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas.
10. Final Provisions
10.1. The Procedure is reviewed at least once per year or immediately after relevant applicable law changes or other significant circumstances occur. Where necessary, the relevant amendments are to be made.
These Rules last modified on 09th November, 2026