Personal Data Processing Policy

VISIONARY ANALYTICS

Contents

1. Main Definitions

1.1. Terms used in capital letters in these Rules for the Processing of Personal Data (hereinafter referred to as **the Rules**) have the following meanings, unless the context gives them a different meaning:

1.1.1. **Personal Data** – means any kind of information about a natural person who is identified or who can be identified (Data Subject); a natural person who can be identified is a person who can be directly or indirectly be identified first of all with identifiers as name and surname, personal identification number, location data and an Internet identifier or by one or more attributes of that natural person's physical, physiological, genetic, mental, economic, cultural or social identity;

1.1.2. **Personal Data Breach** – means any kind of security breach resulting in an unintentional or unlawful destruction, loss, alteration, unauthorized disclosure, transfer, storage or other processing of Personal Data or unauthorized access thereto;

1.1.3. **Personal Data Processing** – means any kind of any operation or sequence of operations on personal data or sets of personal data by automated or non-automated means, such as collection, recording, sorting, systematisation, storage, adaptation or modification, retrieval, access, use, disclosure by transfer, distribution or otherwise access to them, as well as comparison or merging with other data, restrictions, deletion or destruction.

1.1.4. **General Data Protection Regulation** – means 27 April 2016 Regulation (EU) 2019/679 of the European Parliament and 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;

1.1.5. **Company and / or Data Controller** – means UAB "Visionary Analytics", a joint stock company established in accordance with the laws of the Republic of Lithuania, the registered office of which is located at M. Valančius Str. 1A, Vilnius, Republic of Lithuania, legal entity code is 302740632, data about which is collected and stored in the Register of Legal Entities;

1.1.6. **Employee** – means a person of the Company who is an employee of the Company, who has entered into an employment relation with the Company, including the director of the Company;

1.1.7. **Data Subject** – means a natural person, whose data is processed by the Company.

2. Main Provisions

2.1. These rules regulate the functions, rights, and obligations of the Personal Data Controller (Company) in processing Personal Data, as well as determine the rights of Data Subjects, risk factors of personal data protection violation, personal data protection implementation measures and other issues related to Personal Data processing.

2.2. Personal data must be accurate, relevant and not excessive in relation to the collection and further processing of such data. If necessary for the processing of Personal Data, Personal Data may be updated.
2.3. The processing of Personal Data for purposes other than those for which the personal data was originally collected should only be allowed if the processing is compatible with the purposes for which the Personal Data was originally collected.

3. The List of Processed Personal Data and the Purposes of the Personal Data Processing

3.1. The purposes of Personal Data processing:
- 3.1.1. for research purposes;
- 3.1.2. for statistical purposes;
- 3.1.3. for social and public opinion research purposes;
- 3.1.4. for the purposes of administering the database of job candidates (CVs);
- 3.1.5. for internal administrative purposes.

3.2. For the purposes specified in Clause 3.1 (i-iii) of the Rules, the Data Controller shall process the following data:
- 3.2.1. name, surname;
- 3.2.2. workplace;
- 3.2.3. age;
- 3.2.4. occupation or profession;
- 3.2.5. education;
- 3.2.6. address;
- 3.2.7. email;
- 3.2.8. additional data depending on the specific aims of the project.

3.3. When administrating the database of candidates for jobs (CV), the Data Controller processes the following data:
- 3.3.1. name, surname;
- 3.3.2. personal identification number;
- 3.3.3. date of birth;
- 3.3.4. age;
- 3.3.5. email address;
- 3.3.6. address;
- 3.3.7. education;
- 3.3.8. phone number;
- 3.3.9. work experience;
- 3.3.10. foreign languages;
- 3.3.11. ability to work with computer;
- 3.3.12. a candidate’s recommendation and motivational letter, where there is information about the candidate’s ongoing or past work functions, competencies, personal traits;
- 3.3.13. a person’s who recommends the candidate contact information (email, phone number);
- 3.3.14. other information that the candidate decides to disclose (e.g., hobbies, etc).

3.4. For the purposes of internal administration, the Company processes the following Personal Data of the Company's employees: name, surname, personal identification number, date of birth, social security number, gender, address, place of work, profession, experience in the profession, harmful work environment factors and their magnitude in a specific workplace, photo, children's names, personal identification numbers, salary and related taxes, information on leave, information on

concluding and terminating the employment contract, information on business trips, correspondence on staff matters, information on labour disputes, details of another workplace, where an employee of the Company is employed.

4. Legal Bases for the Processing of Personal Data

4.1. All Personal Data must be processed only with the prior consent of the processing of Personal Data, except in the case of processing of anonymous information, i.e. information which does not relate to an identified or identifiable natural person or Personal Data the anonymity of which is ensured, the identity of the Data Subject cannot or can no longer be established, including but not limited to the processing of anonymous information, including for statistical or research purposes.

4.2. Consent should be given in a clear act confirming that there has been a voluntary, specific, informed and unambiguous indication that the Data Subject consents to the processing of Personal Data relating to them, such as in writing, including by electronic means or orally. Silence, pre-ticked boxes or omissions cannot be considered as consent.

4.3. The Company may use, including, but not limited to, one of the following methods of obtaining consent:

- 4.3.1. signing a written statement of consent;
- 4.3.2. by ticking a box for consent in paper or electronic form;
- 4.3.3. by clicking on a consent link or button on the Internet;
- 4.3.4. choosing from equally visible yes / no options;
- 4.3.5. by replying to an email requesting consent (if the Company has the right to send such letters).

4.4. Where the data subject's consent is given in a written statement relating to other matters, the request for consent shall be made in such a way that it is clearly distinguishable from other matters, in a comprehensible and easily accessible form, in clear and simple language.

4.5. The Office Manger shall be responsible for compiling records of consent, which shall include information such as:

- 4.5.1. who agreed (person's name or other identifier);
- 4.5.2. when they agreed (a copy of a document stating the date or electronic records with a time stamp, notes with the date of the consent given orally);
- 4.5.3. what was stated at the time (original document or data submission form including the consent notice used at the time, together with any separate privacy policy, including version numbers and dates corresponding to the date the consent was given. If the consent was given orally - a copy of the standard text, script used at that time);
- 4.5.4. how the consent was given (in the case of written consent, this would be a copy of the document or data collection form. If consent was given online, the records should include both the data provided and the timestamp for linking to the relevant data collection form. If oral consent was given, audio records should be kept, but it does not have to be a record of the whole interview/talk);
- 4.5.5. whether consent has been withdrawn, if so, when.

4.6. In order to obtain a Data Subject's consent to process their Personal Data for research purposes, the Company must provide the Data Subject with sufficient information to make a voluntary statement of the Data Subject's will (e.g. from which sources Personal Data will be collected, the nature of the investigation, its tasks, the institution where the investigation is conducted, the employee of the Company conducting the investigation, whether the results of the investigation will be published, etc.).

4.7. Where a Data Subject's consent is given in a written statement relating to other matters, the request for consent shall be made in such a way that it is clearly distinguishable from other matters, in a comprehensible and easily accessible form, in clear and simple language.

4.8. The consent should cover all Personal Data processing activities carried out for the same purpose or purposes. Where data is processed for more than one purpose, consent should be given for all purposes of the processing. If the consent of the Data Subject is requested electronically, the request shall be clear, concise and not unnecessarily interrupt the use of the service for which the consent is sought.

4.9. A Data Subject from whom the Personal Data is collected may, at its discretion, cooperate with the Company or refuse to cooperate. They should be given the right to withdraw further cooperation at any stage of an investigation, without giving any reason. If the Data Subject refuses to cooperate, the Personal Data of this Data Subject must be destroyed.

4.10. A Data Subject shall have the right to withdraw their consent at any time, unless the processing is necessary for the performance of a task carried out for reasons of public interest. Withdrawal of consent does not affect the lawfulness of the consent-based processing of Personal Data carried out before the withdrawal of consent. The Data Subject shall be informed before consent is given. Withdrawal of consent must be as easy as giving it.

4.11. The protection of Personal Data is organized, ensured, and performed by the Director of the Company and / or an Employee authorized by the Director of the Company.

4.12. When Personal Data is processed for statistical purposes, the statistical results may be further used for a variety of purposes, including research. A statistical purpose means that the result of data processing for statistical purposes is not Personal Data but aggregated Personal Data, and hence that result or Personal Data is not used in making measures or decisions concerning a natural person.

5. Requirements for Individuals Who Process Personal Data

5.1. Access to Personal Data may be granted only to employees, affiliated experts or external experts hired to carry out particular tasks in a project, subcontractors or partners that carry out specific tasks under a contractual agreement, for whom Personal Data is necessary for the performance of their functions.

5.2. Only those actions for which the individual is entitled to perform may be performed with Personal Data.

5.3. The individual processing Personal Data must:

5.3.1. comply with the basic requirements for the personal data processing and security requirements established in the Law on the Legal Protection of Personal Data of the Republic of Lithuania, these Rules, the General Data Protection Regulation and other legal acts;

5.3.2. observe the principle of confidentiality and keep confidential any information related to Personal Data, which they have accessed in the performance of their functions, unless such information is public in accordance with the provisions of applicable laws or other legal acts. The obligation to maintain the confidentiality of Personal Data is indefinite, even in the event of termination of the employment relationship with the Company;

5.3.3. comply with the organizational and technical security measures for Personal Data set out in these Rules in order to prevent accidental or unlawful destruction, alteration, disclosure of

Personal Data, as well as any other unlawful processing, storage of documents, data files and data stored in databases and avoid unnecessary copying;

5.3.4. not disclose, transfer or create conditions for access to Personal Data by any means to any person who is not authorized to process the Personal Data;

5.3.5. immediately notify their direct manager of any suspicious situation that may pose a threat to the security of Personal Data processed by the Company;

5.3.6. take interest in topical issues and problems of Personal Data protection, moreover, if there is a Personal Data;

5.3.7. comply with other requirements established in these Rules and legal acts regulating the protection of Personal Data.

6. Data Subject Identification and Requests

6.1. A Data Subject has the right to exercise all their rights as a Personal Data Subject by submitting an identity document to the Company or in accordance with the procedure established by legal acts or by electronic means of communication that allow proper identification of a person who has confirmed their identity. If the Data Subject's request is sent by post or a courier, it must be accompanied by a copy of the applicant's identity document certified by a notary or a lawyer representing the Data Subject.

6.2. The Company should use all reasonable means to verify the identity of a Data Subject, in particular in relation to Internet services and Internet identifiers.

6.3. The Data Controller shall, without undue delay, but in any case no later than one month after receipt of the request, provide a Data Subject with information on the action taken on their request. That period may be extended by two more months, if necessary, depending on the complexity and number of applications. The Company must inform the Data Subject of such an extension within one month of receiving the request, together with the reasons for the delay.

6.4. The Company may charge a reasonable fee, based on administrative costs, for any copies requested by a Data Subject.

6.5. Where a Data Subject's requests are manifestly unfounded or disproportionate, in particular because of their repetitive content, the Company may charge a reasonable fee based on the administrative costs of providing the information or notifications or actions requested, or may refuse to act on the request. It will be for the company to prove that the request is manifestly unfounded or disproportionate.

6.6. If the Company fails to act on a Data Subject's request, the Company undertakes to inform the Data Subject immediately, but no later than within one month from the receipt of the Data Subject's request, about the reasons for inaction and the possibility to contact the State Data Protection Inspectorate.

7. Right to Access Personal Data

7.1. A Data Subject must have the right to access the Personal Data collected about them and to be able to exercise that right easily and at reasonable intervals in order to be aware of the processing of Personal Data and to verify its lawfulness. Every Data Subject has the right to know and be informed, in particular as to the purposes for which Personal Data is processed and, if possible, the period for which it is processed, who the recipients of the data are.

7.2. Upon request to the Company, a Data Subject has the right to receive confirmation whether the Personal Data related them is processed, and if such Personal Data is processed, they have the right to access the Personal Data and the following information:
  7.2.1. purposes of Personal Data processing;
  7.2.2. relevant categories of Personal Data;
  7.2.3. recipients or categories of recipients to whom the Personal Data has been or will be disclosed, in particular recipients in or international organizations;
  7.2.4. where possible, the period for which the personal data will be stored or, if that is not possible, the criteria for determining that period;
  7.2.5. the right to request the Data Controller to rectify or delete Personal Data or to restrict the processing of Personal Data related to the Data Subject or to object to such processing;
  7.2.6. the right to lodge a complaint with the supervisory authority;
  7.2.7. when Personal Data is collected from outside the Data Subject, all available information on their sources;
  7.2.8. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information on its rationale, as well as the significance of such data processing and the expected consequences for the Data Subject.

8. Right to Request the Deletion of Data ("Right to Be Forgotten")

8.1. A Data Subject has the right to demand that the Company deletes Personal Data related to them without undue delay, and the Company is obliged to delete the Personal Data without undue delay, if this can be justified by one of the following reasons:
  8.1.1. Personal Data is no longer necessary to achieve the purposes for which it was collected or otherwise processed;
  8.1.2. The Data Subject revokes the consent on the basis of which the processing of Personal Data is based, and there is no other legal basis for processing the Personal Data;
  8.1.3. Personal data was processed illegally;
  8.1.4. Personal Data must be deleted in accordance with the legal obligation established by the law of the European Union or a Member State applicable to the Company.

8.2. Nevertheless, the exercise of the Data Subject's right to be "forgotten" is absolute and may be limited in at least one of the following circumstances:
  8.2.1. to exercise the right to freedom of expression and information;
  8.2.2. a legal obligation requiring the processing to be imposed in order to comply with European Union or Member State law applicable to the Data Controller, or for the performance of a task carried out in the public interest or in the exercise of official authority conferred on the Data Controller;
  8.2.3. for reasons of public interest in the field of public health;
  8.2.4. for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes, where the "right to be forgotten" may make it impossible or seriously jeopardize the achievement of the purposes of that processing;
  8.2.5. to make, enforce or defend legal claims.

9. Right to Dispute the Processing of Personal Data

9.1. A Data Subject has the right to object to the processing of Personal Data relating to him at any time in the following cases:

9.1.1. when Personal Data is processed for the performance of a task carried out in the public interest or in the exercise of public authority or the processing of the Personal Data is necessary for the legitimate interests of the Data Controller or a third party, including profiling;

9.1.2. when Personal Data is processed for direct marketing purposes, including profiling insofar as it relates to such direct marketing. Direct marketing is an activity designed to offer goods or services directly to individuals and / or to seek their opinion on the goods or services offered;

9.1.3. in the case of using information society services, the Data Subject may not consent to the use of automated processing of Personal Data in relation to his / her Personal Data;

9.1.4. when Personal Data is processed for scientific or historical research or statistical purposes, except where the processing of personal data is necessary for the performance of a task carried out for reasons of public interest.

10. Right to Request the Correction of Personal Data

10.1. A Data Subject also has the right, upon submission of an identity document and a request to the Data Controller (by post or e-mail), to request the deletion of his / her Personal Data when the Personal Data has been processed in violation of legal acts and / or these Rules.

10.2. A Data Subject should have the right to demand the rectification of their Personal Data and the right to be forgotten when the storage of such Personal Data violates the General Data Protection Regulation, the Law on Legal Protection of Personal Data of the Republic of Lithuania and / or other legal acts applicable to the Data Controller.

10.3. A Data Subject has the right to request that his / her Personal Data be deleted and no longer processed when:

10.3.1. Personal Data is no longer needed for the purposes for which it was collected or otherwise processed when the Data Subject has withdrawn their consent or do not consent to the processing of their personal data; or

10.3.2. The processing of Personal Data for other reasons does not comply with the requirements of the General Data Protection Regulation.

10.4. In order for a Data Subject to have better control over their Personal Data, the Data Subject must also be allowed to obtain the Personal Data relating to them that they have provided to the Company in a structured, commonly used, computer-readable and interoperable format and transfer it to another Data Controller.

10.5. A Data Subject also has the right, upon request for to the Data Controller (by post or e-mail), to request the suspension or rectification of the processing of their Personal Data. Upon suspension of the processing of their Personal Data, the processing of Personal Data which has been suspended, shall be stored until it is rectified or destroyed (at the request of the Data Subject or after the expiry of the

term of storage of Personal Data). Other processing operations with such Personal Data may be performed only:

10.5.1. for the purpose of proving the circumstances due to which the processing of Personal Data has been suspended;

10.5.2. if the Data Subject gives consent to further process their Personal Data;

10.5.3. if necessary to protect the rights or legitimate interests of third parties.

11. Direct Marketing Measures

11.1. The use of electronic communications services, including sending e-mails, for the purpose of direct marketing shall be permitted only with the prior consent of the Data Subject.

11.2. Any communication (e.g. sending an e-mail, making a call) in order to obtain consent to make direct marketing offers is not possible during the communication without the consent of the Data Subject.

11.3. It is strictly forbidden to send e-mails or make calls to a Data Subject asking if they agree to receive direct marketing offers. The Data Subject's prior consent to the use of Personal Data for direct marketing purposes must be obtained in other ways (e.g. by expressing consent on the website, concluding a contract, filling in various forms).

11.4. The Company must provide Data Subjects with an exhaustive list of processed Personal Data, as well as specify the specific recipients of the Data to whom the Personal Data may be transferred. Data Subjects must also be informed that the list of recipients of Personal Data is subject to change and will be kept up to date.

11.5. A Data Subject should be able to choose whether they wish to receive information about changes to the list, and if so, by what means (e.g. e-mails, etc.). In addition, the Data Subject must also be able to consent not only to the processing of their Personal Data for the purpose of direct marketing, but also to refuse or subsequently withdraw the given consent.

11.6. If Personal Data is processed for direct marketing purposes, the Data Subject should have the right to object to such processing at any time, free of charge, including profiling insofar as it relates to such direct marketing, whether initial or further processing. That right should be clearly communicated to the Data Subject and this information should be provided clearly and separately from all other information.

11.7. Where the Data Subject objects to the processing of Personal Data for direct marketing purposes, Personal Data may not be processed for such purposes.

12. Personal Data Transfer

12.1. Personal Data may be transferred (provided) to other persons only in the cases and according to the procedure provided for in the applicable legal acts. Personal Data is transferred (provided) only in the Republic of Lithuania and (or) to other European Union countries.

12.2. If there is a need for the Personal Data Controllers to transfer the Personal Data processed by them to third parties, the Personal Data shall be transferred to them in accordance with the procedure established by legal acts.

13. Data Controller

13.1. The Company commits to use only such Data Processors who provide sufficient guarantees, in particular with expert knowledge, reliability and resources, to implement technical and organizational measures, so that the processing of Personal Data complies with the General Data Protection Regulation and the Republic of Lithuania requirements of the Law on Legal Protection of Data and ensure adequate protection of the rights of the Data Subject.

13.2. The processing of Personal Data by the Data Processor shall be governed by an agreement which shall specify, inter alia, the subject matter and duration of the processing of Personal Data, the nature and purpose of the processing, the type of Personal Data and the categories of Data Subjects, obligations and rights of the Data Controller.

13.3. That contract or other provision of law shall provide, in particular, that the Data Processor shall include, but not be limited to:

13.3.1. processing Personal Data only in accordance with the instructions documented by the Data Controller, including those related to the transfer of personal data to a third country or an international organization;

13.3.2. ensuring that the persons authorized to process Personal Data are bound by an obligation of confidentiality or are subject to an appropriate obligation of confidentiality laid down in the statutes;

13.3.3. at the choice of the Data Controller, upon completion of the provision of services related to data processing, deleting or returning to the Data Controller all Personal Data and deleting the existing copies thereof, except in cases when legal acts require the storage of Personal Data;

13.3.4. providing the Data Controller with all information necessary to prove that the Data Controller fulfils its obligations and facilitates and assists the Data Controller or another auditor authorized by the Data Controller to perform audits, including inspections;

13.3.5. upon learning about Personal Data security violation, unreasonably immediately, but not later than after 3 (three) hours, notify the Data Controller in writing.

14. Measures for the Implementation of Personal Data Protection

14.1. In order to ensure the protection of Personal Data, a Personal Data Controller implements or intends to implement the following Personal Data Protection Measures:

14.1.1. organizational (acquaintance of employees with the documents regulating to data security, periodic review of documents regulating to data security, updating if necessary; their implementation is controlled); and

14.1.2. hardware and software protection.

14.2. Protection against unauthorized physical access to computer equipment:

14.2.1. locked premises;

14.2.2. equipped with premises monitoring and alarm system.

14.3. Protection against users of illegal software:

14.3.1. established user login procedure;

14.3.2. managed user access to the software.

14.4. Theft protection:

14.4.1. limited access to physical data;

14.4.2. personal Data is not stored on personal computers;
14.4.3. restricted software access to data.
14.5. Protection against data network misuse:
14.5.1. data transmission network management programs are run;
14.5.2. strict network routes are established;
14.5.3. the status of the data transmission network is monitored.
14.6. Software error protection:
14.6.1. use of certified software;
14.6.2. the modified software is tested on a separate server or servers.
14.7. Malware protection:
14.7.1. antivirus software installed on the servers, the servers are periodically scanned with antivirus software;
14.7.2. antivirus software is installed on personal computers;
14.7.3. staff are introduced to procedures for dealing with an influx of malware.
14.8. Protection against media destruction:
14.8.1. a procedure for recovering data from backup media is foreseen.
14.9. Protection against illegal software use:
14.9.1. only legitimate software is used;
14.9.2. continuous control of the software used in personal computers;
14.9.3. employees are not entitled to install the software themselves.
14.10. User error protection:
14.10.1. employees are trained to work with software;
14.10.2. accurate and detailed work instructions provided for Employees.
14.11. Protection against computer hardware failure:
14.11.1. the equipment is maintained in accordance with the manufacturer's recommendations; maintenance and troubleshooting is performed by qualified specialists;
14.11.2. the most important computer equipment is duplicated;
14.11.3. the technical condition of the most important computer equipment is constantly monitored.
14.12. Flood protection:
14.12.2. properly designed and equipped storage facilities for critical computer equipment;
14.12.3. equipped with water detection and drainage system.
14.13. Fire protection:
14.13.1. there are fire extinguishers in the premises of the building;
14.13.2. smoke and heat sensors installed in the premises;
14.13.3. allocated smoking areas for Employees.
14.14. Protection against matting and communication line failure
14.14.1 the cables are in insulating wires;
14.14.2. electrical and data cables are securely separated.

14.15. The Company periodically, but at least twice a year, performs testing of managed information systems, including databases, during which the reliability of the Company's servers and information systems, resistance to congestion, resistance to cyber-attacks, viruses, and other factors threatening the reliability of the system are checked. Personal Data is not used during testing of company-managed systems.
14.16. The Company makes copies of the data in the active database at least once a day, which are stored in the passive database. Access to the passive database is granted only to the system administrator appointed by the Company's director, who in case of emergency data loss restores the last copies of the Company's data database within 48 hours of data loss from the passive database.

14.17. The Company provides uninterrupted and autonomous power supply to the servers where the active and passive databases are stored; the servers are stored in the premises where the fire and security alarm system is installed. The premises are locked and cannot be accessed by unauthorized persons.
14.18. All Employees who have the right to process Personal Data or to organize and enforce their protection must strictly comply with these Rules and legislation governing the legal protection of personal data.

15. Personal Data Management Terms

15.1. A Personal Data Controller processes the Personal Data for the following period:
  15.1.1. for the purposes of research Personal Data is stored for two years;
  15.1.2. for the purposes of statistical research Personal Data is stored for two years;
  15.1.3. for the purposes of social and public opinion research Personal Data is stored for one year.
15.2. When the deadline for processing the Personal Data expires, the Personal Data is securely destroyed. Also, Personal Data is immediately and securely destroyed if the Data Subject revokes their consent to the processing of Personal Data or the Company has a reasonable suspicion to believe that the illegal use of Personal Data needs to be prevented.
15.3. Personal Data may be stored for a longer period than specified in these Rules at the Company's discretion, if there is reason to believe that Personal Data may be required for the investigation of a criminal offense or other incident at the Company's premises or in the building containing the premises (for example, natural disasters) or any other event that caused damage to the Company. In this case, the Personal Data is stored until an appropriate law enforcement or court decision related to a criminal act or other person investigating the incident (e.g. insurers in case of natural disasters) or other persons investigating the event causing damage to the Company is made, decision or conclusion.

16. Responsibility

16.1. Liability measures provided in the laws of the Republic of Lithuania shall apply to the Company's director and (or) Employees authorized by the director processing Personal Data in the Republic of Lithuania that violates the requirements of the Law on Legal Protection of Personal Data of the Republic of Lithuania, other legal acts regulating the processing and protection of Personal Data or these Rules.

17. Policy Introduction Procedure

17.1. Each Employee is acquainted with the Rules in the following order:
  17.1.1. immediately after approval of the Rules, the Rules are sent to all existing Employees by e-mail;
  17.1.2. immediately after the approval of the Rules, the Rules are placed on the Company's server (or in another place where all the Company's internal memoranda, procedures and rules are stored) and are available to the Employees there at any time;
  17.1.3. each new Employee is acquainted with the Rules on the first day of their work in the Company by submitting the Rules to them by e-mail or providing access to the Rules at the place specified in the clause (ii).

18. Final Provisions

18.1. Compliance monitoring and, if necessary, review, is entrusted to the representatives of the Personal Data Controllers or their authorized Employees. The Rules are reviewed (updated as necessary) every 24 (twenty-four) months, or when the legislation governing the processing and protection of Personal Data changes;

18.2. Enquiries about this Policy or the use of Personal Data can be sent to contact@visionary.lt.