

---

## WEBSITE PRIVACY POLICY

---

### **1. GENERAL PROVISIONS**

- 1.1. This Privacy Policy (hereinafter referred to as the Policy) governs the principles and procedure of processing of personal data, as well as the conditions of the operation of the website [www. lituaniacantat.it](http://www.lituaniacantat.it) (hereinafter referred to as the Website) maintained by the Data Controller.

- 1.2. The Data Subject in this Policy is any natural person whose personal data is processed by the Data Controller.
- 1.3. The Data Controller guarantees that, when adopting and implementing this Policy, the Data Controller seeks to implement the following essential principles related to the processing of personal data:
  - (a) The Data Controller aims to ensure that personal data is processed in a lawful, fair and transparent manner in respect to the Data Subject (the principle of lawfulness, fairness and transparency);
  - (b) The Data Controller aims to collect personal data for specified, clearly defined and legitimate purposes and to further prevent the processing of the data in a way incompatible with those purposes; the further processing of personal data for archiving purposes in favour of the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the original objectives (the principle of purpose limitation);
  - (c) The Data Controller aims to ensure that personal data is adequate, relevant and only such as necessary to achieve the purposes for which it is being processed (the principle of data reduction);
  - (d) The Data Controller aims and all efforts shall be made to ensure that personal data is accurate and updated as necessary within the reasonable time from the change of the data; it is intended to take all reasonable steps to ensure that personal data which is not accurate in the light of the purposes for which the data is processed would be immediately deleted or corrected within a reasonable time (the principle of accuracy);
  - (e) The Data Controller aims to store personal data in a form that allows identification of the personal identity of Data Subjects for no longer than necessary for the purposes for which personal data is processed; personal data may be stored for more extended periods when personal data is only processed for archival purposes in favour of the public interest, scientific or historical research or statistical purposes, by implementing the appropriate technical and organizational measures necessary to protect the rights and freedoms of the Data Subject (the principle of storage limitation);
  - (f) The Data Controller aims to ensure that personal data, taking into account the generic nature of the personal data processed by the Data Controller, is processed in such a way that with the use of appropriate technical or organizational measures the proper security of personal data is ensured, including protection against unauthorized processing of personal data or unauthorized personal data processing, or accidental loss, destruction or damage of personal data (the principle of integrity and confidentiality);
  - (g) The Data Controller shall be responsible for complying with the principles mentioned above and must be able to demonstrate that these principles are being followed (the principle of accountability).
- 1.4. By using the services of third-parties, for example, when visiting the account of the Data Controller on the social network Facebook, the terms of third parties may apply. For example, Facebook applies its data policy to all its users and visitors. Therefore, when using the services of third parties, it is recommended to familiarise with their terms and conditions.

- 1.5. This Policy is based on 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 (hereinafter referred to as GDPR), the Law on the Legal Protection of Personal Data of the Republic of Lithuania (hereinafter referred to as LLPPD), other legal acts of the European Union and the Republic of Lithuania. The definitions used in this Policy shall be understood as defined by GDPR and LLPPD.

## **2. COLLECTION, PROCESSING AND STORAGE OF PERSONAL DATA**

- 2.1. By submitting his/her personal data, the Data Subject agrees and does not oppose to the management and processing of the personal data by the Data Controller for the purposes, by the means and following the procedures provided for in this Policy and legislation.
- 2.2. If the Data Subject disagrees with this Policy and the processing of personal data described therein, he/she should not visit the Website and/or use the services of the Data Controller.
- 2.3. By submitting his/her personal data, the Data Subject grants the Data Controller the right to collect, compile, organise, use and process for the purpose provided for in this Policy all personal data that the Data Subject provides directly or indirectly through the Website and using its services.
- 2.4. The Data Subject shall be responsible for ensuring that the data provided by him/her is accurate, correct and complete. Entering of knowingly incorrect data is considered a violation of the Policy. If the submitted data changes, the Data Subject must immediately correct them, and in the absence of the possibility to do so, inform the Data Controller accordingly. Under no circumstances will the Data Controller be liable for damages caused to the Data Subject and/or third parties due to the fact that the Data Subject has provided incorrect and/or incomplete personal data or did not apply regarding the supplement and/or modification of the data upon their change.

## **3. PROCESSING OF PERSONAL DATA FOR THE PURPOSE OF RESPONDING TO THE REQUESTS OF DATA SUBJECTS**

- 3.1. The Data Controller shall automatically process the following personal data of the Data Subjects who have given such consent for the purpose of responding to the inquiries of Data Subjects:
  - (a) Name and surname;
  - (b) E-mail;
  - (c) Phone number;
  - (d) Information provided by the Data Subject relating to the cause and results of the investigations launched and completed by pre-trial investigation authorities or the criminal, civil and administrative proceedings before the court, and disclosing such data as the name, gender, address of residence of the Data Subject, his/her personal identification number, contact phone number, e-mail address, workplace and address of employer, state plate number of the vehicle driven, data on the health status of the Data subject, bank account number, bank name,

other information related solely to specific legal services ordered by the Data Subject.

(e) Other information provided voluntarily by the Data Subject.

3.2. The data shall be received directly from the Data Subject and shall not be transmitted to third parties.

3.3. The legal basis for the processing of personal data is Article 6 P(1)(a) of the GDPR (the processing of data carried out subject to the consent of the Data subject).

#### **4. PROCEDURE AND TERMS OF STORAGE OF PERSONAL DATA**

4.1. While processing and storing the personal data of Data Subjects, the Data Controller implements organisational and technical measures aimed to ensure the protection of personal data against accidental or unlawful destruction, alteration, disclosure, as well as any other unlawful processing.

4.2. The Data Controller applies the following terms for the storage of personal data:

Purpose of personal data processing	Term of storage
Response to inquiries of Data Subjects	As long as the data is needed to assess the prospects of the provision of services, and after considering the prospects and after the conclusion of a service contract - 5 (five) years from the date from the termination or expiry on other grounds of the agreement of legal services or representation concluded with the Data Subject.

4.3. Exceptions from the above-mentioned storage terms may be determined to the extent that such deviations do not violate the rights of the Data Subjects, comply with legal requirements, are adequately documented and to the extent justified by the legitimate interests of the Data Controller or third party.

4.4. The data necessary for the filing, enforcement or defence of legal claims shall be protected insofar as they are necessary to achieve such purposes with the use of a judicial, administrative or extrajudicial procedure.

#### **5. DESTRUCTION OF DATA**

5.1. Personal data shall be stored to the extent required by the terms and purposes of the processing of data. Where personal data is no longer required for the purpose of processing and/or when the time limit for the processing of personal data provided for in the Policy expires, the personal data must be destroyed unconditionally.

5.2. Destruction is defined as a physical or technical act by which personal data contained in a document is made unrecoverable by conventional commercially available means.

5.3. Personal data stored in an electronic form shall be destroyed by deleting it without the ability to restore it.

5.4. Paper documents containing personal data shall be shredded, and the paper waste shall

be discarded safely.

## **6. RIGHTS OF DATA SUBJECTS**

- 6.1. Data subjects have the right at any time, upon filing a request to the Data Controller, to familiarise with their personal data processed by the Data Controller and to find out how they are processed, to request to correct incorrect, incomplete, inaccurate personal data, to demand to suspend, except for storage, the processing of personal data when the data is processed in breach of the laws and this Policy.
- 6.2. To the extent that the processing of personal data is based on the consent, the Data Subject has the right at any time to withdraw the consent without affecting the lawfulness of the processing of the data that had been processed on the grounds of the consent before the withdrawal of the consent.
- 6.3. The Data Subject may make use of his/her rights by submitting a written request by e-mail [info@lituaniacantat.lt](mailto:info@lituaniacantat.lt)
- 6.4. If the Data Subject is not satisfied with the response of the Data Controller or believes that the Data Controller processes the personal data of the Data Subject without complying with legal requirements, the Data Subject may submit a complaint to the State Data Protection Inspectorate of the Republic of Lithuania.

## **7. TECHNICAL AND ORGANIZATIONAL DATA PROTECTION MEASURES**

- 7.1. The organisational and technical personal data protection measures implemented by the Data Controller shall provide such level of protection that is consistent with the nature of the personal data managed by the Data Controller and the risks associated with the processing of such personal data.
- 7.2. The Data Controller's employees shall observe the principle of confidentiality and shall keep confidential any personal data that they have familiarised with in the course of their duties unless such information is public in accordance with the provisions of applicable laws or regulations.
- 7.3. Access to the copies of personal data recorded in a computer system in digital formats shall be password protected.
- 7.4. Access to personal data and the right to perform personal data processing operations shall be granted only to those responsible employees who need access to personal data in accordance with their duties and work functions.
- 7.5. In order to protect the automated processing of personal data, the following technical data protection measures shall be used:
  - (a) The responsible employees shall use unique passwords for access to personal data, which will be changed and protected to ensure their confidentiality;
  - (b) Protection of the processed personal data against unauthorised access to the electronic computer network by means of electronic communication shall be ensured;
  - (c) The use of secure protocols and passwords when personal data is transmitted through external personal data networks shall be ensured;

- (d) The protection of computer hardware against malicious software (installation, updating of antivirus software, etc.) shall be ensured.
- 7.6. The Data Controller seeks to implement the appropriate technical and organisational measures to ensure standardised processing of the personal data necessary for each specific purpose only. This obligation applies to the amount of personal data collected, the scope of their processing, the storage period and the availability. In particular, such measures shall ensure that no unlimited numbers of natural persons can access personal data in a standardised way, without the intervention of a natural person.
- 7.7. The Data Controller shall take the necessary precautionary measures to protect the integrity of the personal data of Data Subjects and to prevent such personal data from being damaged or lost, including the provision of the necessary retrieval of personal data.

## **8. FINAL PROVISIONS**

- 8.1. The legal relations related to this Policy shall be governed by the law of the Republic of Lithuania.
- 8.2. The Data Controller shall not be liable for damage, including the damage resulting from interruptions to the use of the Website, the loss or damage to data resulting from the acts or omissions of the person or third parties acting with the person's knowledge, mistakes, deliberate damage or another misuse of the Website. In addition, the Data Controller shall not be responsible for any interruption and/or disturbances of the use of the Website or the damage caused by them resulting from the actions or omissions of third parties not related to the Data Controller or the person, including electrical, Internet access disruptions, etc.
- 8.3. The Data Controller has the right to modify the Policy in whole or in part.
- 8.4. The supplements or amendments of the Policy shall take effect from the day they are published on the Website.
- 8.5. If, after a supplement or amendment of the Policy, the person continues to use the Website and/or the services provided by the Data Controller, the person shall be deemed not to be contradicting to such supplements and/or amendments.