Annex 1

1. The Company shall have a personal data protection policy, i.e. personal data protection rules (the "**Rules**"), that set the procedures of personal data processing, monitoring and eliminating of any potential breaches; General Manager's order(s) approving the Rules and appointing respective employees responsible for data protection security in the company; list of company's employees acknowledged with the Rules; other internal documentation regulating the personal data protection matters;

2. Implemented procedure regarding evaluation of the personal data being processed by the Company. The Company shall assign the personal data collected and processed to the specific security level, periodically monitor the processed personal data, specify and select measures that are mandatory to implement in order to ensure the required technical security level and that are chosen depending on the categories of the processed personal data (the aforementioned measures should be set in the Rules or separate internal document). The detailed requirements are set in the *State Personal Data Protection Inspectorate Director's order issued on 12 November 2008 No. 1t-12(1.12)*

   <https://www.e-tar.lt/portal/lt/legalAct/b79f22e086c011e481c9c95e73113964/DUrypCPGSb>;

3. The Company shall be registered with the Personal Data Processors Register (applicable until 25 May 2017);

4. The Company shall regularly organise the data protection related trainings in order to increase the staff's awareness about GDPR provisions or inform its managers and employees about the personal data protection legislation requirement applied to the Company in any other appropriate way;

5. The Company shall have implemented a customer information procedure. This procedure shall be designated to inform the customers (physical persons) about the status of personal data processor and the reason(s) for processing of their personal data;

6. In case the Company carries out a direct marketing, the Company shall implement the process that would ensure obtaining a written consent from the customers in advance. Also this procedure shall ensure that the consent of the customer could be easily withdrawn upon the customer's will;

7. The Company shall seek to ensure the safety of the personal data processing, management and control (e.g. the confidentiality of the data processing systems should be ensured by authorising only the respective persons to access the specific systems or physically access the personal data processed by the Company);

8. The Company shall guarantee implementation of physical safety measures in the company (e.g. to limit the number of the people entering the premise where files are being kept physically);

9. The countries to which the personal data processed by the Company is being transferred shall be identified. The measures ensuring the same safe data transferring (sending and receiving) and storing conditions (i.e. the requirements same as applied in the member state where the Company is established) shall be applied.