EU and non-EU companies

Clause of the contract to be entered into between the Controller and the Processor

Upon entry into and performance of the contract, the parties consider themselves to be bound by the General Data Protection Regulation (GDPR) approved by the European Parliament on 14 April 2016 regardless of whether the territory or country they are located in has adopted the GDPR or equivalent legislation. Upon performing the contract, the parties shall follow in their activities in more detail the duties and obligations of the Processor described in Articles 27 and 28 of the GDPR, as well as the definitions used and rules established in the GDPR.

The Processor may not process personal data in any other manner or for any other reason than on the basis and within the framework of the powers conferred by the Controller. If the activities of the Processor require designation of a data protection officer, the Processor shall designate such an officer.

Upon maintaining a register of processing of personal data specified in Article 30(2) of the GDPR, the Processor shall record the processing of personal data within the framework of the powers conferred by the Controller in a manner that allows for presenting the data free of charge, immediately and without impediments to the Controller or to the supervisory authority (the Estonian Data Protection Inspectorate).

Upon processing of personal data, the Processor shall, in order to ensure the performance of the contract, implement appropriate and technical means to ensure the level of security corresponding to the risk, and also be capable of verifying the implementation of measures that address the risk. The Processor shall notify its employees of the need for a high level of protection of personal data under the contract entered into with the Controller and ensure that its employees have the right and proper understanding and expertise for processing personal data in accordance with the GDPR. The Processor shall without delay notify the Controller of any personal data breach and the notice must contain the information provided in Article 33(3) of the GDPR.

Upon performing the contract, the Processor shall, among other things, adhere in its activities to the following principles established by the GDPR: the lawfulness, fairness and transparency of processing of personal data (Article 5(1)(a) and Article 6), the principle of purpose limitation (Article 5(1)(b)), the principle of data minimisation (Article 5(1)(c)), the principle of accuracy (Article 5(1)(d)), storage limitation (Article 5(1)(e)), integrity and confidentiality (Article 5(1)(f)), special need for protecting the personal data of children (Article 8) and special categories of personal data (Article 9), security of processing personal data (Article 32), general principles for transfers of personal data (Article 44).

In addition, the Processor shall, when engaging another Processor, adhere to Article 28(2) (conditions for engaging) and Article 28(4) (regulation of data protection obligations upon engaging), Article 28(3) (conditions for engaging that must have been regulated either in legislation or a contract), including but not limited to: the mandatory nature of regulation of the obligation of confidentiality (Article 28(3)(b)), the mandatory nature of the obligation to assist (Article 28(3)(e)), and assisting the Controller in the performance of the Controller’s obligations such as the obligation of secure processing (Article 32), the obligation to notify the supervisory authority (Article 33), the obligation to communicate a breach to the data subject (Article 34), the obligation to carry out a data protection impact assessment (Article 35), and the obligation to consult the supervisory authority prior to processing (Article 36).

The Processor shall immediately comply with any orders of the Controller in relation to personal data, including those that have been issued for the processing, alteration, deletion, transfer, restriction of processing or the return of personal data. The Processor is also obliged to assist the Controller if the need for such assistance arises from supervision proceedings that are being conducted or may be conducted with respect to the Controller.

The Processor shall avoid the Controller incurring any damage or causing any damage to the Controller and compensate for any damage, claims, fines and penalty payments that arise or are filed against the Controller and have been caused due to the Processor directly or indirectly failing to comply with the requirements of the GDPR or the partial compliance therewith.

The Processor shall return and delete personal data without an additional order if the data are no longer needed for the provision of services or for ensuring the performance of other obligations arising from legislation. In such instances, the Processor shall provide prior notice to the Controller of the respective activities. If the Processor needs to enter into a contract for the delegation of powers for the purpose of the lawful processing of personal data, the respective contract shall, given the scope of the powers of the Controller, also establish clear liability based on the GDPR with regard to the Processor who acts on the basis of the delegation of powers.