**Article - Commercial Law**

[Previous][Next]

§14–4708.

(a) (1) If a controller uses a processor to process the personal data of consumers, the controller and the processor shall enter into a contract that governs the processor's data processing procedures with respect to processing performed on behalf of the controller.

(2) The contract shall be binding and shall clearly set forth:

(i) Instructions for processing data;

(ii) The nature and purpose of processing;

(iii) The type of data subject to processing;

(iv) The duration of processing; and

(v) The rights and obligations of both parties.

(3) The contract shall require that the processor:

(i) Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the personal data;

(ii) Establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data, considering the volume and nature of the personal data;

(iii) Stop processing data on request by the controller made in accordance with a consumer's authenticated request;

(iv) At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of service, unless retention of the personal data is required by law;

(v) On the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in this subtitle;

(vi) After providing the controller an opportunity to object, engage a subcontractor to assist with processing personal data on the controller's behalf only in accordance with a written contract that requires the subcontractor to meet the processor's obligations regarding the personal data under the processor's contract with the controller; and

(vii) Allow and cooperate with reasonable assessments by the controller, the controller's designated assessor, or a qualified and independent assessor arranged for by the processor to assess the processor's policies and technical and organizational measures in support of the obligations under this subtitle.

(4) (i) On request, the processor shall provide a report of an assessment required by paragraph (3)(v) of this subsection to the controller.

(ii) An assessment conducted in accordance with paragraph (3)(v) of this subsection shall be conducted using an appropriate and accepted control standard or framework and assessment procedure for the assessments.

(b) A processor shall:

(1) Adhere to the contract and instructions of a controller;

(2) Assist the controller in meeting the controller's obligations under this subtitle, including:

(i) By appropriate technical and organizational measures as much as reasonably practicable to fulfill the controller's obligation to respond to consumer rights requests, considering the nature of processing and the information available to the processor; and

(ii) By assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of a system, as defined in § 14–3504 of this title; and

(3) Provide necessary information to enable the controller to conduct and document data protection assessments.

(c) Nothing in this section may be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship in accordance with this section.

(d) (1) The determination of whether a person is acting as a controller or a processor with respect to a specific processing of data is a fact–based determination that depends on the context in which personal data is being processed.

(2) A person is considered to be a controller if the person:

(i) Is not limited in the person's processing of specific personal data in accordance with a controller's instructions; or

(ii) Fails to adhere to a controller's instructions with respect to a specific processing of personal data.

(3) A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor.

(4) If a processor or third party begins, alone or jointly with others, determining the purposes and means of the processing of personal data, the processor:

(i) Is a controller with respect to the processing; and

(ii) May be subject to an enforcement action under this subtitle.

(e) Nothing in this section may be construed to alter a controller's obligation to limit a person's processing of personal data or to take steps to ensure that a processor adheres to the controller's instructions.

[Previous][Next]