casetext
Part of Thomson Reuters

Colo. Rev. Stat. § 6-1-1305

Section 6-1-1305 - Responsibility according to role

(1) Controllers and processors shall meet their respective obligations established under this part 13.

(2) Processors shall adhere to the instructions of the controller and assist the controller to meet its obligations under this part 13. Taking into account the nature of processing and the information available to the processor, the processor shall assist the controller by:

(a) Taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 6-1-1306;

(b) Helping to meet 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 the system pursuant to section 6-1-716; and

(c) Providing information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 6-1-1309. The controller and processor are each responsible for only the measures allocated to them.

(3) Notwithstanding the instructions of the controller, a processor shall:

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

(b) Engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract in accordance with subsection (5) of this section that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

(4) Taking into account the context of processing, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures.

(5) Processing by a processor must be governed by a contract between the controller and the processor that is binding on both parties and that sets out:

(a) The processing instructions to which the processor is bound, including the nature and purpose of the processing;

(b) The type of personal data subject to the processing, and the duration of the processing;

(c) The requirements imposed by this subsection (5) and subsections (3) and (4) of this section; and

(d) The following requirements:

casetext
Part of Thomson Reuters

(I) At the choice of the controller, the processor shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(II)

(A) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations in this part 13; and

(B) The processor shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, the processor may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at the processor's expense, an audit of the processor's policies and technical and organizational measures in support of the obligations under this part 13 using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable. The processor shall provide a report of the audit to the controller upon request.

(6) In no event may a contract relieve a controller or a processor from the liabilities imposed on them by virtue of its role in the processing relationship as defined by this part 13.

(7) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data are to be processed. A person that is not limited in its processing of personal data pursuant to a controller's instructions, or that fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with others, determining the purposes and means of the processing of personal data, it is a controller with respect to the processing.

(8)

(a) A controller or processor that discloses personal data to another controller or processor in compliance with this part 13 does not violate this part 13 if the recipient processes the personal data in violation of this part 13, and, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation.

(b) A controller or processor receiving personal data from a controller or processor in compliance with this part 13 as specified in subsection (8)(a) of this section does not violate this part 13 if the controller or processor from which it receives the personal data fails to comply with applicable obligations under this part 13.

C.R.S. § 6-1-1305

Added by 2021 Ch. 483, § 1, eff. 7/1/2023.

casetext
Part of Thomson Reuters