Effective 12/31/2023

Part 3
Requirements for Controllers and Processors

13-61-301 Responsibility according to role.

(1) A processor shall:

(a) adhere to the controller's instructions; and

(b) taking into account the nature of the processing and information available to the processor, by appropriate technical and organizational measures, insofar as reasonably practicable, assist the controller in meeting the controller's obligations, including obligations related to the security of processing personal data and notification of a breach of security system described in Section 13-44-202.

(2) Before a processor performs processing on behalf of a controller, the processor and controller shall enter into a contract that:

(a) clearly sets forth instructions for processing personal data, the nature and purpose of the processing, the type of data subject to processing, the duration of the processing, and the parties' rights and obligations;

(b) requires the processor to ensure each person processing personal data is subject to a duty of confidentiality with respect to the personal data; and

(c) requires the processor to engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the same obligations as the processor with respect to the personal data.

(3)

(a) 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.

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

Enacted by Chapter 462, 2022 General Session

13-61-302 Responsibilities of controllers -- Transparency -- Purpose specification and data minimization -- Consent for secondary use -- Security -- Nondiscrimination -- Nonretaliation -- Nonwaiver of consumer rights.

(1)

(a) A controller shall provide consumers with a reasonably accessible and clear privacy notice that includes:

(i) the categories of personal data processed by the controller;

(ii) the purposes for which the categories of personal data are processed;

(iii) how consumers may exercise a right;

(iv) the categories of personal data that the controller shares with third parties, if any; and

(v) the categories of third parties, if any, with whom the controller shares personal data.

(b) If a controller sells a consumer's personal data to one or more third parties or engages in targeted advertising, the controller shall clearly and conspicuously disclose to the consumer the manner in which the consumer may exercise the right to opt out of the:

(i) sale of the consumer's personal data; or

(ii) processing for targeted advertising.

(2)
(a) A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to:
(i) protect the confidentiality and integrity of personal data; and
(ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing of personal data.
(b) Considering the controller's business size, scope, and type, a controller shall use data security practices that are appropriate for the volume and nature of the personal data at issue.
(3) Except as otherwise provided in this chapter, a controller may not process sensitive data collected from a consumer without:
(a) first presenting the consumer with clear notice and an opportunity to opt out of the processing; or
(b) in the case of the processing of personal data concerning a known child, processing the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's implementing regulations and exemptions.
(4)
(a) A controller may not discriminate against a consumer for exercising a right by:
(i) denying a good or service to the consumer;
(ii) charging the consumer a different price or rate for a good or service; or
(iii) providing the consumer a different level of quality of a good or service.
(b) This Subsection (4) does not prohibit a controller from offering a different price, rate, level, quality, or selection of a good or service to a consumer, including offering a good or service for no fee or at a discount, if:
(i) the consumer has opted out of targeted advertising; or
(ii) the offer is related to the consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.
(5) A controller is not required to provide a product, service, or functionality to a consumer if:
(a) the consumer's personal data are or the processing of the consumer's personal data is reasonably necessary for the controller to provide the consumer the product, service, or functionality; and
(b) the consumer does not:
(i) provide the consumer's personal data to the controller; or
(ii) allow the controller to process the consumer's personal data.
(6) Any provision of a contract that purports to waive or limit a consumer's right under this chapter is void.

Enacted by Chapter 462, 2022 General Session

13-61-303 Processing deidentified data or pseudonymous data.
(1) The provisions of this chapter do not require a controller or processor to:
(a) reidentify deidentified data or pseudonymous data;
(b) maintain data in identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data; or
(c) comply with an authenticated consumer request to exercise a right described in Subsections 13-61-202(1) through (3), if:
(i)

(A) the controller is not reasonably capable of associating the request with the personal data; or
(B) it would be unreasonably burdensome for the controller to associate the request with the personal data;
(ii) the controller does not:
(A) use the personal data to recognize or respond to the consumer who is the subject of the personal data; or
(B) associate the personal data with other personal data about the consumer; and
(iii) the controller does not sell or otherwise disclose the personal data to any third party other than a processor, except as otherwise permitted in this section.
(2) The rights described in Subsections 13-61-201(1) through (3) do not apply to pseudonymous data if a controller demonstrates that any information necessary to identify a consumer is kept:
(a) separately; and
(b) subject to appropriate technical and organizational measures to ensure the personal data are not attributed to an identified individual or an identifiable individual.
(3) A controller who uses pseudonymous data or deidentified data shall take reasonable steps to ensure the controller:
(a) complies with any contractual obligations to which the pseudonymous data or deidentified data are subject; and
(b) promptly addresses any breach of a contractual obligation described in Subsection (3)(a).

Enacted by Chapter 462, 2022 General Session

13-61-304 Limitations.
(1) The requirements described in this chapter do not restrict a controller's or processor's ability to:
(a) comply with a federal, state, or local law, rule, or regulation;
(b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, local, or other governmental entity;
(c) cooperate with a law enforcement agency concerning activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;
(d) investigate, establish, exercise, prepare for, or defend a legal claim;
(e) provide a product or service requested by a consumer or a parent or legal guardian of a child;
(f) perform a contract to which the consumer or the parent or legal guardian of a child is a party, including fulfilling the terms of a written warranty or taking steps at the request of the consumer or parent or legal guardian before entering into the contract with the consumer;
(g) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual;
(h)
(i) detect, prevent, protect against, or respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any illegal activity; or
(ii) investigate, report, or prosecute a person responsible for an action described in Subsection (1)(h)(i);
(i)
(i) preserve the integrity or security of systems; or
(ii) investigate, report, or prosecute a person responsible for harming or threatening the integrity or security of systems, as applicable;

(j) if the controller discloses the processing in a notice described in Section 13-61-302, engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws;
(k) assist another person with an obligation described in this subsection;
(l) process personal data to:
(i) conduct internal analytics or other research to develop, improve, or repair a controller's or processor's product, service, or technology;
(ii) identify and repair technical errors that impair existing or intended functionality; or
(iii) effectuate a product recall;
(m) process personal data to perform an internal operation that is:
(i) reasonably aligned with the consumer's expectations based on the consumer's existing relationship with the controller; or
(ii) otherwise compatible with processing to aid the controller or processor in providing a product or service specifically requested by a consumer or a parent or legal guardian of a child or the performance of a contract to which the consumer or a parent or legal guardian of a child is a party; or
(n) retain a consumer's email address to comply with the consumer's request to exercise a right.
(2) This chapter does not apply if a controller's or processor's compliance with this chapter:
(a) violates an evidentiary privilege under Utah law;
(b) as part of a privileged communication, prevents a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under Utah law; or
(c) adversely affects the privacy or other rights of any person.
(3) A controller or processor is not in violation of this chapter if:
(a) the controller or processor discloses personal data to a third party controller or processor in compliance with this chapter;
(b) the third party processes the personal data in violation of this chapter; and
(c) the disclosing controller or processor did not have actual knowledge of the third party's intent to commit a violation of this chapter.
(4) If a controller processes personal data under an exemption described in Subsection (1), the controller bears the burden of demonstrating that the processing qualifies for the exemption.
(5) Nothing in this chapter requires a controller, processor, third party, or consumer to disclose a trade secret.

Enacted by Chapter 462, 2022 General Session

13-61-305 No private cause of action.

A violation of this chapter does not provide a basis for, nor is a violation of this chapter subject to, a private right of action under this chapter or any other law.

Enacted by Chapter 462, 2022 General Session