Information Accountability Foundation

U.S. State Assessment Provisions v.1.0 (June 2023)

California (*July 1, 2023, rules TBA*)

As part of its rulemaking responsibilities, the Agency is directed to do the following pursuant to Civil Code § 1798.185(a)(15)-(16):

(15) Issu[e] regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

> (A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.
>
> (B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

(16) Issu[e] regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer

Colorado (*July 1, 2023*)

PART 8 DATA PROTECTION ASSESSMENTS

Rule 8.01 AUTHORITY AND PURPOSE

A. The statutory authority for the rules in this Part 8 is C.R.S. §§ 6-1-108(1), 6-1-1309, and 6-1-1313. The purpose of the rules in this Part 8 is to provide clarity on the requirements and timing of data protection assessments.

Rule 8.02 SCOPE

A. A data protection assessment shall be a genuine, thoughtful analysis of each Personal Data Processing activity that presents a heightened risk of harm to a Consumer, pursuant to C.R.S. § 6-1-1309(3), that: 1) identifies and describes the risks to the rights of consumers associated with the processing; 2) documents measures considered and taken to address and offset those risks, including

those duties required by C.R.S. § 6-1-1308; 3) contemplates the benefits of the Processing; and 4) demonstrates that the benefits of the Processing outweigh the risks offset by safeguards in place.

B. If a Controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

1. If a data protection assessment conducted for the purpose of complying with another jurisdiction's law or regulation is not similar in scope and effect to a data protection assessment created pursuant to this section, a Controller may submit that assessment with a supplement that contains any additional information required by this jurisdiction.

C. The depth, level of detail, and scope of data protection assessments should take into account the scope of risk presented, the size of the Controller, amount and sensitivity of Personal Data Processed, Personal Data Processing activities subject to the assessment, and complexity of safeguards applied.

D. A "comparable set of Processing operations" that can be addressed by a single data protection assessment pursuant to C.R.S. § 6-1-1309(5) is a set of similar Processing operations including similar activities that present heightened risks of similar harm to a Consumer.

1. Example: The ACME Toy Store chain is considering using in-store paper forms to collect names, mailing addresses, and birthdays from Children that visit their stores, and using that information to mail a coupon and list of age-appropriate toys to each child during the Child's birth month and every November. ACME uses the same Processors and Processing systems for each category of mailings across all stores. ACME must conduct and document a data protection assessment because it is Processing Personal Data from known Children, which is Sensitive Data. ACME can use the same data protection assessment for Processing the Personal Data for the birthday mailing and November mailing across all stores because in each case it is collecting the same categories of Personal Data in the same way for the purpose of sending coupons and age-appropriate toy lists to Children.

Rule 8.03 STAKEHOLDER INVOLVEMENT

A data protection assessment shall involve all relevant internal actors from across the Controller's organizational structure, and where appropriate, relevant external parties, to identify, assess and address the data protection risks.

Rule 8.04 DATA PROTECTION ASSESSMENT CONTENT

A. At a minimum, a data protection assessment must include the following information:

1. A short summary of the Processing activity;
2. The categories of Personal Data to be Processed and whether they include Sensitive Data, including Personal Data from a known Child as described in C.R.S. § 6-1-1303(24);
3. The context of the Processing activity, including the relationship between the Controller and the Consumers whose Personal Data will be Processed, and the reasonable expectations of those Consumers;
4. The nature and operational elements of the Processing activity. In determining the level of detail and specificity to provide pursuant to this section, the Controller shall consider the type, amount, and sensitivity of Personal Data Processed, the impacts that operational elements will

have on the level of risk presented by the Processing activity, and any relevant unique relationships. Relevant operational elements may include:

a. Sources of Personal Data;

b. Technology or Processors to be used;

c. Names or categories of Personal Data recipients, including Third Parties, Affiliates, and Processors that will have access to the Personal Data, the processing purpose for which the Personal Data will be provided to those recipients, and categorical compliance processes that the Controller uses to evaluate that type of recipient;

d. Operational details about the Processing, including planned processes for Personal Data collection, use, storage, retention, and sharing;

e. Specific types of Personal Data to be processed

5. The core purposes of the Processing activity, as well as other benefits of the Processing that may flow, directly and indirectly to the Controller, Consumer, other expected stakeholders, and the public;

6. The sources and nature of risks to the rights of Consumers associated with the Processing activity posed by the Processing activity. The source and nature of the risks may differ based on the processing activity and type of Personal Data processed. Risks to the rights of Consumers that a Controller may consider in a data protection assessment include, for example, risks of:

a. Constitutional harms, such as speech harms or associational harms;

b. Intellectual privacy harms, such as the creation of negative inferences about an individual based on what an individual reads, learns, or debates;

c. Data security harms, such as unauthorized access or adversarial use;

d. Discrimination harms, such as a violation of federal antidiscrimination laws or antidiscrimination laws of any state or political subdivision thereof, or unlawful disparate impact;

e. Unfair, unconscionable, or deceptive treatment;

f. A negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services;

g. Financial injury or economic harm;

h. Physical injury, harassment, or threat to an individual or property;

i. Privacy harms, such as physical or other intrusion upon the solitude or seclusion or the private affairs or concerns of Consumers, stigmatization or reputational injury;

j. Psychological harm, including anxiety, embarrassment, fear, and other mental trauma; or CODE OF COLORADO REGULATIONS 4 CCR 904-3 Department of Law – Consumer Protection 38

k. Other detrimental or negative consequences that affect an individual's private life, private affairs, private family matters or similar concerns, including actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used.

7. Measures and safeguards the Controller will employ to reduce the risks identified by the Controller pursuant to 4 CCR 904-3, Rule 8.04(A)(6). Measures shall include the following, as applicable:

a. The use of De-identified Data;

b. Measures taken pursuant to the Controller duties in C.R.S. § 6-1-1308, including an overview of data security practices the Controller has implemented, any data security assessments that have been completed pursuant to C.R.S. § 6-1- 1308(5), and any measures taken to comply with the consent requirements of 4 CCR 904-3, Rule 7; and

c. Measures taken to ensure that Consumers have access to the rights provided in C.R.S. § 6-1-1306.

8. A description of how the benefits of the Processing outweigh the risks identified pursuant to 4 CCR 904-3, Rule 8.04(A)(6), as mitigated by the safeguards identified pursuant to 4 CCR 904-3, Rule 8.04(A)(7).

a. Contractual agreements in place to ensure that Personal Data in the possession of a Processor or other Third Party remains secure; or

b. Any other practices, policies, or trainings intended to mitigate Processing risks.

9. If a Controller is Processing Personal Data for Profiling as contemplated in C.R.S. § 6-1-1309(2)(a), a data protection assessment of that Processing activity must also comply with 4 CCR 904-3, Rule 9.06;

10. If a Controller is Processing Sensitive Data pursuant to the exception in section 4 CCR 904-3, Rule 6.10, the details of the process implemented to ensure that Personal Data and Sensitive Data Inferences are not transferred and are deleted within twenty-four (24) hours of the Personal Data Processing activity;

11. Relevant internal actors and external parties contributing to the data protection assessment;

12. Any internal or external audit conducted in relation to the data protection assessment, including, the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process; and

13. Dates the data protection assessment was reviewed and approved, and names, positions, and signatures of the individuals responsible for the review and approval.

Rule 8.05 TIMING

A. A Controller shall conduct and document a data protection assessment before initiating a Processing activity that Presents a Heightened Risk of Harm to a Consumer, as defined at C.R.S. § 6-1-1309(2).

B. A Controller shall review and update the data protection assessment as often as appropriate considering the type, amount, and sensitivity of Personal Data Processed and level of risk presented by the Processing, throughout the Processing activity's lifecycle in order to: 1) monitor for harm caused by the Processing and adjust safeguards accordingly; and 2) ensure that data protection and privacy are considered as the Controller makes new decisions with respect to the Processing.

C. Data protection assessments containing Processing for Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer shall be reviewed and updated at least annually, and include an updated evaluation for fairness and disparate impact and the results of any such evaluation.

D. A new data Processing activity is generated when existing Processing activities are modified in a way that materially changes the level of risk presented. When a new data Processing activity is generated, a data protection assessment must reflect changes to the pre-existing activity and additional considerations and safeguards to offset the new risk level.

1. Modifications that may materially change the level of risk of a Processing activity may include, without limitation, changes to any of the following:

a. The way that existing systems or Processes handle Personal Data;
b. Processing purpose;
c. Personal data Processed or sources of Personal Data;
d. Method of collection of Personal Data;
e. Personal Data recipients;
f. Processor roles or Processors;
g. Algorithm applied or algorithmic result; or
h. Software or other systems used for Processing.

E. Data protection assessments, including prior versions which have been revised when a new data Processing activity is generated, shall be stored for as long as the Processing activity continues, and for at least three (3) years after the conclusion of the Processing activity. Data protection assessments shall be held in an electronic, transferable form.

F. Data protection assessments shall be required for activities created or generated after July 1, 2023. This requirement is not retroactive.

Rule 8.06 ATTORNEY GENERAL REQUESTS

A. A Controller shall make the data protection assessment available to the Attorney General within thirty (30) days of the Attorney General's request.

Connecticut (*July 1, 2023*)

Sec. 8. (NEW) (Effective July 1, 2023)

(a) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:

(1) The processing of personal data for the purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers,

(B) financial, physical or reputational injury to consumers,

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or

(D) other substantial injury to consumers; and

(4) the processing of sensitive data.

(b) Data protection assessments conducted pursuant to subsection (a) of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The controller shall factor into any such data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

(c) The Attorney General may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in sections 1 to 11, inclusive, of this act. Data protection assessments shall be confidential and shall be exempt from disclosure under the Freedom of Information Act, as defined in section 1-200 of the general statutes. To the extent any information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, such disclosure shall not constitute a waiver of such privilege or protection.

(d) A single data protection assessment may address a comparable set of processing operations that include similar activities.

(e) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

(f) Data protection assessment requirements shall apply to processing activities created or generated after July 1, 2023, and are not retroactive.

Florida (*July 1, 2023*)

501.713 Data protection assessments.—

(1) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(a) The processing of personal targeted advertising.

(b) The sale of personal data.

(c) The processing of personal profiling if the profiling presents risk of:

data for purposes of a reasonably foreseeable

1. Unfair or deceptive treatment of or unlawful disparate impact on consumers;

2. Financial, physical, or reputational injury to consumers;

3. A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or

4. Other substantial injury to consumers.

(d) The processing of sensitive data.

(e) Any processing activities involving personal data which present a heightened risk of harm to consumers.

(2) A data protection assessment conducted under subsection (1) must do all of the following:

(a) Identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce such risks.

(b) Factor into the assessment:

1. The use of deidentified data;
2. The reasonable expectations of consumers;
3. The context of the processing; and
4. The relationship between the controller and the consumer whose personal data will be processed.

(3) The disclosure of a data protection assessment in compliance with a request from the Attorney General pursuant to s. 501.72 does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(4) A single data protection assessment may address a comparable set of processing operations which include similar activities.

(5) A data protection assessment conducted by a controller for the purpose of compliance with any other law or regulation may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.

(6) This section applies only to processing activities generated on or after July 1, 2023.

Indiana (*January 1, 2026*)

Chapter 6. Data Protection Impact Assessments

Sec. 1.

(a) The data protection impact assessment requirements set forth in this chapter apply to processing activities created or generated after December 31, 2025, and are not retroactive to any processing activities created or generated before January 1, 2026.

(b) A controller shall conduct and document a data protection impact assessment of each of the following processing activities involving personal data:

(1) The processing of personal data for purposes of targeted advertising.

(2) The sale of personal data.

(3) The processing of personal data for purposes of profiling, if such profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, if such intrusion would be offensive to a reasonable person; or

(D) other substantial injury to consumers.

(4) The processing of sensitive data.

(5) Any processing activities involving personal data that present a heightened risk of harm to consumers.

(c) Data protection impact assessments conducted under this chapter shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

(d) A single data protection impact assessment may address a comparable set of processing operations that include similar activities.
(e) A data protection impact assessment conducted by a controller for the purpose of compliance with other laws or regulations may be used to comply with this section if the assessment has a reasonably comparable scope and effect to an assessment conducted under this section.

Sec. 2.
(a) The attorney general may request, pursuant to a civil investigative demand, that a controller disclose any data protection impact assessment that is relevant to an investigation conducted by the attorney general. Upon receipt of such a request, the controller shall make the data protection impact assessment available to the attorney general. Subject to subsection (b), the attorney general may evaluate the data protection impact assessment for a controller's compliance with the responsibilities set forth in IC 24-15-4.
(b) Data protection impact assessments are confidential and exempt from public inspection and copying under IC 5-14-3-4. The disclosure of a data protection impact assessment pursuant to a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

Montana (*January 1, 2025*)

Section 9. Data protection assessment.
(1) A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, processing that presents a heightened risk of harm to a consumer includes:
(a) the processing of personal data for the purposes of targeted advertising;
(b) the sale of personal data;
(c) the processing of personal data for the purposes of profiling in which the profiling presents a reasonably
    (i) foreseeable risk of:
    unfair or deceptive treatment of or unlawful disparate impact on consumers;
    financial, physical, or reputational injury to consumers;
    (ii) a physical or other form of intrusion on the solitude or seclusion or the private affairs or
    (iii) concerns of consumers in which the intrusion would be offensive to a reasonable person; or
    (iv) other substantial injury to consumers; and
(d) the processing of sensitive data.
(2)
(a) Data protection assessments conducted pursuant to subsection (1) must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing as mitigated by safeguards that may be employed by the controller to reduce these risks.
(b) The controller shall factor into any data protection assessment the use of deidentified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.
(3)
(a) The attorney general may require that a controller disclose any data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller shall make the data protection assessment available to the attorney general.
(b) The attorney general may evaluate the data protection assessment for compliance with the responsibilities set forth in [sections 1 through 12].

(c) Data protection assessments are confidential and are exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552.
(d) To the extent any information contained in a data protection assessment disclosed to the attorney general includes information subject to attorney-client privilege or work product protection, the disclosure may not constitute a waiver of the privilege or protection.
(4) A single data protection assessment may address a comparable set of processing operations that include similar activities.
(5) If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment must be considered to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.
(6) Data protection assessment requirements must apply to processing activities created or generated after January 1, 2025, and are not retroactive.

Tennessee (*July 1, 2024*)

DATA PROTECTION ASSESSMENTS

This bill requires a controller to conduct and document a data protection assessment of each of the following processing activities involving personal information:

(1) The processing of personal information for purposes of targeted advertising;

(2) The sale of personal information;

(3) The processing of personal information for purposes of profiling, where the profiling presents a reasonably foreseeable risk of:

(A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(B) Financial, physical, or reputational injury to consumers;

(C) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or

(D) Other substantial injury to consumers;

(4) The processing of sensitive data; and

(5) Processing activities involving personal information that present a heightened risk of harm to consumers.

The data protection assessments conducted must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by the safeguards that can be employed by the controller to reduce the risks.

The attorney general is authorized to request that a controller disclose the data protection assessment that is relevant to an investigation conducted by the attorney general, and the controller must then make the assessment available. The attorney general is also authorized to evaluate the assessment for compliance with the responsibilities set forth by this bill. Data protection assessments are confidential

and not open to public inspection and copying.

This bill provides that data protection assessment requirements apply to processing activities created or generated on or after July 1, 2024, and are not retroactive.

Texas (*March 1, 2024*)

Sec.54.105. DATA PROTECTION ASSESSMENTS.

(a) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(1) the processing of personal data for purposes of targeted advertising;

(2) the sale of personal data;

(3) the processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of:

(A) unfair or deceptive treatment of or unlawful disparate impact on consumers;

(B) financial, physical, or reputational injury to consumers;

(C) a physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or

(D)other substantial injury to consumers;

(4) the processing of sensitive data; and

(5) any processing activities involving personal data that present a heightened risk of harm to consumers.

(b) data protection assessment conducted under Subsection (a) must:

(1) identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce the risks; and

(2) factor into the assessment:

(A) the use of deidentified data;

(B) the reasonable expectations of consumers;

(C)the context of the processing; and

(D) the relationship between the controller and the consumer whose personal data will be processed.

(c) controller shall make a data protection assessment requested under Section 541.153(b) available to the attorney general pursuant to a civil investigative demand under Section 541.153.

(d) data protection assessment is confidential and exempt from public inspection and copying under Chapter 552, Government Code. Disclosure of a data protection assessment in compliance with a request from the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(e) single data protection assessment may address a comparable set of processing operations that include similar activities.

(f) data protection assessment conducted by a controller for the purpose of compliance with other laws or regulations may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.

Virginia

59.1-580. (*January 1, 2023*) Data protection assessments.

A. A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

1. The processing of personal data for purposes of targeted advertising;

2. The sale of personal data;

3. The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers;

4. The processing of sensitive data; and

5. Any processing activities involving personal data that present a heightened risk of harm to consumers.

B. Data protection assessments conducted pursuant to subsection A shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

C. The Attorney General may request, pursuant to a civil investigative demand, that a controller disclose any data protection assessment that is relevant to an investigation conducted by the Attorney General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in § 59.1-578. Data protection assessments shall be confidential and exempt from public inspection and copying under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.). The disclosure of a data protection assessment pursuant to a request from the Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.
D. A single data protection assessment may address a comparable set of processing operations that include similar activities.

E. Data protection assessments conducted by a controller for the purpose of compliance with other laws or regulations may comply under this section if the assessments have a reasonably comparable scope and effect.

F. Data protection assessment requirements shall apply to processing activities created or generated after January 1, 2023, and are not retroactive.

2021, Sp. Sess. I, cc. 35, 36.