A BILL FOR AN ACT

CONCERNING ADDITIONAL PROTECTION OF DATA RELATING TO PERSONAL PRIVACY.

Bill Summary

(Note: This summary applies to this bill as introduced and does not reflect any amendments that may be subsequently adopted. If this bill passes third reading in the house of introduction, a bill summary that applies to the reengrossed version of this bill will be available at http://leg.colorado.gov.)

The bill creates personal data privacy rights and:

- Applies to legal entities that conduct business or produce products or services that are intentionally targeted to Colorado residents and that either:
  - Control or process personal data of more than 100,000 consumers per calendar year; or
Derive revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers; and

Does not apply to personal data governed by listed state and federal laws, listed activities, and employment records.

Consumers have the right to opt out of the processing of their personal data; access, correct, or delete the data; or obtain a portable copy of the data. The bill defines a "controller" as a person that, alone or jointly with others, determines the purposes and means of processing personal data. A "processor" means a person that processes personal data on behalf of a controller.

The bill:

• Specifies how controllers must fulfill duties regarding consumers' assertion of their rights, transparency, purpose specification, data minimization, avoiding secondary use, care, avoiding unlawful discrimination, and sensitive data;

• Requires controllers to conduct a data protection assessment for each of their processing activities involving personal data that present a heightened risk of harm to consumers, such as processing for purposes of targeted advertising or processing sensitive data; and

• May be enforced only by the attorney general or district attorneys.

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1. In Colorado Revised Statutes, add part 13 to article 1 of title 6 as follows:

PART 13

COLORADO PRIVACY ACT

6-1-1301. Short title. The short title of this Part 13 is the "COLORADO PRIVACY ACT".

6-1-1302. Legislative declaration. (1) The general assembly hereby:

(a) Finds that:

(I) The people of Colorado regard their privacy as a fundamental right and an essential element of their individual
FREEDOM:

(II) Colorado’s constitution explicitly provides the right to privacy under section 7 of article II, and fundamental privacy rights have long been, and continue to be, integral to protecting Coloradans and to safeguarding our democratic republic:

(III) Ongoing advances in technology have produced exponential growth in the volume and variety of personal data being generated, collected, stored, and analyzed and these advances present both promise and potential peril:

(IV) The ability to harness and use data in positive ways is driving innovation and brings beneficial technologies to society, but it has also created risks to privacy and freedom:

and

(V) The unauthorized disclosure of personal information and loss of privacy can have devastating impacts ranging from financial fraud, identity theft, and unnecessary costs in personal time and finances to destruction of property, harassment, reputational damage, emotional distress, and physical harm:

(b) Determines that:

(I) Technological innovation and new uses of data can help solve societal problems and improve lives, and it is possible to build a world where technological innovation and privacy can coexist; and

(II) States across the United States are looking to this part 13 and similar models to enact state-based data privacy
REQUIREMENTS AND TO EXERCISE THE LEADERSHIP THAT IS LACKING AT
THE NATIONAL LEVEL; AND

(c) DECLARES THAT:

(I) BY ENACTING THIS PART 13, COLORADO WILL BE AMONG THE
STATES THAT EMPOWER CONSUMERS TO PROTECT THEIR PRIVACY AND
REQUIRE COMPANIES TO BE RESPONSIBLE CUSTODIANS OF DATA AS THEY
CONTINUE TO INNOVATE;

(II) THIS PART 13 ADDRESSES ISSUES OF STATEWIDE CONCERN
AND:

(A) PROVIDES CONSUMERS THE RIGHT TO ACCESS, CORRECT, AND
DELETE PERSONAL DATA AND THE RIGHT TO OPT OUT NOT ONLY OF THE
SALE OF PERSONAL DATA BUT ALSO OF THE COLLECTION AND USE OF
PERSONAL DATA;

(B) IMPOSES AN AFFIRMATIVE OBLIGATION UPON COMPANIES TO
SAFEGUARD PERSONAL DATA; TO PROVIDE CLEAR, UNDERSTANDABLE, AND
TRANSPARENT INFORMATION TO CONSUMERS ABOUT HOW THEIR PERSONAL
DATA ARE USED; AND TO STRENGTHEN COMPLIANCE AND ACCOUNTABILITY
BY REQUIRING DATA PROTECTION ASSESSMENTS IN THE COLLECTION AND
USE OF PERSONAL DATA; AND

(C) EMPOWERS THE ATTORNEY GENERAL AND DISTRICT
ATTORNEYS TO ACCESS AND EVALUATE A COMPANY’S DATA PROTECTION
ASSESSMENTS, TO IMPOSE PENALTIES WHERE VIOLATIONS OCCUR, AND TO
PREVENT FUTURE VIOLATIONS.

6-1-1303. Definitions. As used in this Part 13, unless the
context otherwise requires:

(1) "Affiliate" means a legal entity that controls, is
CONTROLLED BY, OR IS UNDER COMMON CONTROL WITH ANOTHER LEGAL
ENTITY. AS USED IN THIS SUBSECTION (1), "CONTROL" MEANS:

(a) OWNERSHIP OF, CONTROL OF, OR POWER TO VOTE TWENTY-FIVE
PERCENT OR MORE OF THE OUTSTANDING SHARES OF ANY CLASS OF
VOTING SECURITY OF THE ENTITY, DIRECTLY OR INDIRECTLY, OR ACTING
THROUGH ONE OR MORE OTHER PERSONS;

(b) CONTROL IN ANY MANNER OVER THE ELECTION OF A MAJORITY
OF THE DIRECTORS, TRUSTEES, OR GENERAL PARTNERS OF THE ENTITY OR
OF INDIVIDUALS EXERCISING SIMILAR FUNCTIONS; OR

(c) THE POWER TO EXERCISE, DIRECTLY OR INDIRECTLY, A
CONTROLLING INFLUENCE OVER THE MANAGEMENT OR POLICIES OF THE
ENTITY AS DETERMINED BY THE APPLICABLE PRUDENTIAL REGULATOR, AS
THAT TERM IS DEFINED IN 12 U.S.C. SEC. 5481 (24), IF ANY.

(2) "AUTHENTICATE" MEANS TO USE REASONABLE MEANS TO
determine that a request to exercise any of the rights in section
6-1-1306 (1) is being made by or on behalf of the consumer who is
entitled to exercise the rights.

(3) "BUSINESS ASSOCIATE" HAS THE MEANING ESTABLISHED IN 45
CFR 160.103.

(4) "CHILD" MEANS AN INDIVIDUAL UNDER THIRTEEN YEARS OF
AGE.

(5) "CONSENT" MEANS A CLEAR, AFFIRMATIVE ACT SIGNIFYING A
CONSUMER'S FREELY GIVEN, SPECIFIC, INFORMED, AND UNAMBIGUOUS
AGREEMENT, SUCH AS BY A WRITTEN STATEMENT, INCLUDING BY
ELECTRONIC MEANS, OR OTHER CLEAR, AFFIRMATIVE ACTION BY WHICH
THE CONSUMER SIGNIFIES AGREEMENT TO THE PROCESSING OF PERSONAL
DATA RELATING TO THE CONSUMER FOR A NARROWLY DEFINED
PARTICULAR PURPOSE. THE FOLLOWING DOES NOT CONSTITUTE CONSENT:
(a) Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;

(b) Hovering over, muting, pausing, or closing a given piece of content; and

(c) Agreement obtained through dark patterns.

(6) "Consumer":

(a) Means an individual who is a Colorado resident acting only in an individual or household context; and

(b) Does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context.

(7) "Controller" means a person that, alone or jointly with others, determines the purposes for and means of processing personal data.

(8) "Covered entity" has the meaning established in 45 CFR 160.103.

(9) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice.

(10) "Decisions that produce legal or similarly significant effects concerning a consumer" means a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

(11) "De-identified data" means data that cannot
REASONABLY BE USED TO INFER INFORMATION ABOUT, OR OTHERWISE BE LINKED TO, AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL, OR A DEVICE LINKED TO SUCH AN INDIVIDUAL, IF THE CONTROLLER THAT POSSESSES THE DATA:

(a) TAKES REASONABLE MEASURES TO ENSURE THAT THE DATA CANNOT BE ASSOCIATED WITH AN INDIVIDUAL;

(b) PUBLICLY COMMITS TO MAINTAIN AND USE THE DATA ONLY IN A DE-IDENTIFIED FASHION AND NOT ATTEMPT TO RE-IDENTIFY THE DATA; AND

(c) CONTRACTUALLY OBLIGATES ANY RECIPIENTS OF THE INFORMATION TO COMPLY WITH THE REQUIREMENTS OF THIS SUBSECTION (11).

(12) "HEALTH-CARE FACILITY" MEANS ANY ENTITY THAT IS LICENSED, CERTIFIED, OR OTHERWISE AUTHORIZED OR PERMITTED BY LAW TO ADMINISTER MEDICAL TREATMENT IN THIS STATE.

(13) "HEALTH-CARE INFORMATION" MEANS INDIVIDUALLY IDENTIFIABLE INFORMATION RELATING TO THE PAST, PRESENT, OR FUTURE HEALTH STATUS OF AN INDIVIDUAL.

(14) "HEALTH-CARE PROVIDER" MEANS A PERSON LICENSED, CERTIFIED, OR REGISTERED IN THIS STATE TO PRACTICE MEDICINE, PHARMACY, CHIROPRACTIC, NURSING, PHYSICAL THERAPY, PODIATRY, DENTISTRY, OPTOMETRY, OCCUPATIONAL THERAPY, OR OTHER HEALING ARTS UNDER TITLE 12.


(16) "IDENTIFIED OR IDENTIFIABLE INDIVIDUAL" MEANS AN
INDIVIDUAL WHO CAN BE READILY IDENTIFIED, DIRECTLY OR INDIRECTLY,
IN PARTICULAR BY REFERENCE TO AN IDENTIFIER SUCH AS A NAME, AN
IDENTIFICATION NUMBER, SPECIFIC GEOLOCATION DATA, OR AN ONLINE
IDENTIFIER.

(17) "PERSONAL DATA":
(a) MEANS INFORMATION THAT IS LINKED OR REASONABLY
LINKABLE TO AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL; AND
(b) DOES NOT INCLUDE DE-IDENTIFIED DATA OR PUBLICLY
AVAILABLE INFORMATION. AS USED IN THIS SUBSECTION (17)(b),
"PUBLICLY AVAILABLE INFORMATION" MEANS INFORMATION THAT IS
LAWFULLY MADE AVAILABLE FROM FEDERAL, STATE, OR LOCAL
GOVERNMENT RECORDS AND INFORMATION THAT A CONTROLLER HAS A
REASONABLE BASIS TO BELIEVE THE CONSUMER HAS LAWFULLY MADE
AVAILABLE TO THE GENERAL PUBLIC.

(18) "PROCESS" OR "PROCESSING" MEANS THE COLLECTION, USE,
SALE, STORAGE, DISCLOSURE, ANALYSIS, DELETION, OR MODIFICATION OF
PERSONAL DATA AND INCLUDES THE ACTIONS OF A CONTROLLER
DIRECTING A PROCESSOR TO PROCESS PERSONAL DATA.

(19) "PROCESSOR" MEANS A PERSON THAT PROCESSES PERSONAL
DATA ON BEHALF OF A CONTROLLER.

(20) "PROFILING" MEANS ANY FORM OF AUTOMATED PROCESSING
OF PERSONAL DATA TO EVALUATE, ANALYZE, OR PREDICT PERSONAL
ASPECTS CONCERNING AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL’S
ECONOMIC SITUATION, HEALTH, PERSONAL PREFERENCES, INTERESTS,
RELIABILITY, BEHAVIOR, LOCATION, OR MOVEMENTS.

(21) "PROTECTED HEALTH INFORMATION" HAS THE MEANING
ESTABLISHED IN 45 CFR 160.103.
(22) (a) "Sale", "sell", or "sold" means the exchange of personal data for monetary or other valuable consideration by a controller to a third party.

(b) "Sale", "sell", or "sold" does not include the following:

(I) The disclosure of personal data to a processor that processes the personal data on behalf of a controller;

(II) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(III) The disclosure or transfer of personal data to an affiliate of the controller;

(IV) The disclosure or transfer to a third party of personal data as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets; or

(V) The disclosure of personal data:

(A) That a consumer directs the controller to disclose or intentionally discloses by using the controller to interact with a third party; or

(B) Intentionally made available by a consumer to the general public via a channel of mass media.

(23) "Sensitive data" means:

(a) Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or
CITIZENSHIP STATUS:

(b) GENETIC OR BIOMETRIC DATA THAT MAY BE PROCESSED FOR
THE PURPOSE OF UNIQUELY IDENTIFYING AN INDIVIDUAL; OR

(c) PERSONAL DATA FROM A KNOWN CHILD.

(24) "TARGETED ADVERTISING":

(a) MEANS DISPLAYING TO A CONSUMER AN ADVERTISEMENT THAT
IS SELECTED BASED ON PERSONAL DATA OBTAINED OR INFERRED OVER
TIME FROM THE CONSUMER'S ACTIVITIES ACROSS NONAFFILIATED
WEBSITES, APPLICATIONS, OR ONLINE SERVICES TO PREDICT CONSUMER
PREFERENCES OR INTERESTS; AND

(b) DOES NOT INCLUDE:

(I) ADVERTISING TO A CONSUMER IN RESPONSE TO THE
CONSUMER'S REQUEST FOR INFORMATION OR FEEDBACK;

(II) ADVERTISEMENTS BASED ON ACTIVITIES WITHIN A
CONTROLLER'S OWN WEBSITES OR ONLINE APPLICATIONS;

(III) ADVERTISEMENTS BASED ON THE CONTEXT OF A CONSUMER'S
CURRENT SEARCH QUERY, VISIT TO A WEBSITE, OR ONLINE APPLICATION;
OR

(IV) PROCESSING PERSONAL DATA SOLELY FOR MEASURING OR
REPORTING ADVERTISING PERFORMANCE, REACH, OR FREQUENCY.

(25) "THIRD PARTY" MEANS A PERSON, PUBLIC AUTHORITY,
AGENCY, OR BODY OTHER THAN A CONSUMER, CONTROLLER, PROCESSOR,
OR AFFILIATE OF THE PROCESSOR OR THE CONTROLLER.

6-1-1304. Applicability of part. (1) EXCEPT AS SPECIFIED IN
SUBSECTION (2) OF THIS SECTION, THIS PART 13 APPLIES TO A CONTROLLER
THAT:

(a) CONDUCTS BUSINESS IN COLORADO OR PRODUCES OR DELIVERS
COMMERCIAL PRODUCTS OR SERVICES THAT ARE INTENTIONALLY
TARGETED TO RESIDENTS OF COLORADO; AND
(b) SATISFIES ONE OR BOTH OF THE FOLLOWING THRESHOLDS:
(I) CONTROLS OR PROCESSES THE PERSONAL DATA OF ONE
HUNDRED THOUSAND CONSUMERS OR MORE DURING A CALENDAR YEAR;
OR
(II) DERIVES REVENUE OR RECEIVES A DISCOUNT ON THE PRICE OF
GOODS OR SERVICES FROM THE SALE OF PERSONAL DATA AND PROCESSES
OR CONTROLS THE PERSONAL DATA OF TWENTY-FIVE THOUSAND
CONSUMERS OR MORE.
(2) THIS PART 13 DOES NOT APPLY TO:
(a) PROTECTED HEALTH INFORMATION THAT IS COLLECTED,
STORED, AND PROCESSED BY A COVERED ENTITY OR ITS BUSINESS
ASSOCIATES;
(b) HEALTH-CARE INFORMATION THAT IS GOVERNED BY PART 8 OF
ARTICLE 1 OF TITLE 25 SOLELY FOR THE PURPOSE OF ACCESS TO MEDICAL
RECORDS;
(c) PATIENT IDENTIFYING INFORMATION, AS DEFINED IN 42 CFR
2.11, THAT ARE GOVERNED BY AND COLLECTED AND PROCESSED
PURSUANT TO 42 CFR 2, ESTABLISHED PURSUANT TO 42 U.S.C. SEC.
290dd-2;
(d) IDENTIFIABLE PRIVATE INFORMATION, AS DEFINED IN 45 CFR
46.102, FOR PURPOSES OF THE FEDERAL POLICY FOR THE PROTECTION OF
HUMAN SUBJECTS PURSUANT TO 45 CFR 46; IDENTIFIABLE PRIVATE
INFORMATION THAT IS COLLECTED AS PART OF HUMAN SUBJECTS
RESEARCH PURSUANT TO THE ICH E6 GOOD CLINICAL PRACTICE
GUIDELINE ISSUED BY THE INTERNATIONAL COUNCIL FOR
HARMONISATION OF TECHNICAL REQUIREMENTS FOR PHARMACEUTICALS
FOR HUMAN USE OR THE PROTECTION OF HUMAN SUBJECTS UNDER 21 CFR
50 AND 56; OR PERSONAL DATA USED OR SHARED IN RESEARCH
CONDUCTED IN ACCORDANCE WITH ONE OR MORE OF THE CATEGORIES SET
FORTH IN THIS SUBSECTION (2)(d):

(e) INFORMATION AND DOCUMENTS CREATED BY A COVERED
ENTITY FOR PURPOSES OF COMPLYING WITH HIPAA AND ITS
IMPLEMENTING REGULATIONS:

(f) PATIENT SAFETY WORK PRODUCT, AS DEFINED IN 42 CFR 3.20,
THAT IS CREATED FOR PURPOSES OF PATIENT SAFETY IMPROVEMENT
PURSUANT TO 42 CFR 3, ESTABLISHED PURSUANT TO 42 U.S.C. SECS.
299b-21 TO 299b-26;

(g) INFORMATION THAT IS:

(I) DE-IDENTIFIED IN ACCORDANCE WITH THE REQUIREMENTS FOR
DE-IDENTIFICATION SET FORTH IN 45 CFR 164; AND

(II) DERIVED FROM ANY OF THE HEALTH-CARE-RELATED
INFORMATION DESCRIBED IN THIS SECTION.

(h) INFORMATION MAINTAINED IN THE SAME MANNER AS
INFORMATION UNDER SUBSECTIONS (2)(a) TO (2)(g) OF THIS SECTION BY:

(I) A COVERED ENTITY OR BUSINESS ASSOCIATE;

(II) A HEALTH-CARE FACILITY OR HEALTH-CARE PROVIDER; OR

(III) A PROGRAM OF A QUALIFIED SERVICE ORGANIZATION AS
DEFINED IN 42 CFR 2.11;

(i) (I) EXCEPT AS PROVIDED IN SUBSECTION (2)(i)(II) OF THIS
SECTION, AN ACTIVITY INVOLVING THE COLLECTION, MAINTENANCE,
DISCLOSURE, SALE, COMMUNICATION, OR USE OF ANY PERSONAL DATA
BEARING ON A CONSUMER’S CREDITWORTHINESS, CREDIT STANDING,
CREDIT CAPACITY, CHARACTER, GENERAL REPUTATION, PERSONAL CHARACTERISTICS, OR MODE OF LIVING BY:

(A) A CONSUMER REPORTING AGENCY AS DEFINED IN 15 U.S.C. SEC. 1681a (f);

(B) A FURNISHER OF INFORMATION AS SET FORTH IN 15 U.S.C. SEC. 1681s-2 THAT PROVIDES INFORMATION FOR USE IN A CONSUMER REPORT, AS DEFINED IN 15 U.S.C. SEC. 1681a (d); OR


(j) PERSONAL DATA:

(I) COLLECTED AND MAINTAINED FOR PURPOSES OF ARTICLE 22 OF TITLE 10;

(II) COLLECTED, PROCESSED, SOLD, OR DISCLOSED PURSUANT TO THE FEDERAL "GRAMM-LEACH-BILLEY ACT", 15 U.S.C. SEC. 6801 ET SEQ., AS AMENDED, AND IMPLEMENTING REGULATIONS, IF THE COLLECTION, PROCESSING, SALE, OR DISCLOSURE IS IN COMPLIANCE WITH THAT LAW;

(III) COLLECTED, PROCESSED, SOLD, OR DISCLOSED PURSUANT TO THE FEDERAL "DRIVER'S PRIVACY PROTECTION ACT OF 1994", 18 U.S.C. SEC. 2721 ET SEQ., AS AMENDED, IF THE COLLECTION, PROCESSING, SALE, OR DISCLOSURE IS REGULATED BY THAT LAW;
(IV) REGULATED BY THE FEDERAL "CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998", 15 U.S.C. SECS. 6501 TO 6506, AS AMENDED, IF COLLECTED, PROCESSED, AND MAINTAINED IN COMPLIANCE WITH THAT LAW; OR

(V) REGULATED BY THE FEDERAL "FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974", 20 U.S.C. SEC. 1232g ET SEQ., AS AMENDED, AND ITS IMPLEMENTING REGULATIONS;

(k) DATA MAINTAINED FOR EMPLOYMENT RECORDS PURPOSES;


(m) A NATIONAL SECURITIES ASSOCIATION REGISTERED PURSUANT TO THE FEDERAL "SECURITIES EXCHANGE ACT OF 1934", 15 U.S.C. SEC. 78o-3, AS AMENDED, OR IMPLEMENTING REGULATIONS;

(n) CUSTOMER DATA MAINTAINED BY A PUBLIC UTILITY AS DEFINED IN SECTION 40-1-103 (1)(a)(I) OR AN AUTHORITY AS DEFINED IN SECTION 43-4-503 (1), IF THE DATA ARE NOT COLLECTED, MAINTAINED, DISCLOSED, SOLD, COMMUNICATED, OR USED EXCEPT AS AUTHORIZED BY STATE AND FEDERAL LAW;

(o) INFORMATION USED AND DISCLOSED IN COMPLIANCE WITH 45 CFR 164.512; OR


(3) THE OBLIGATIONS IMPOSED ON CONTROLLERS OR PROCESSORS
UNDER THIS PART 13 DO NOT:

(a) RESTRICT A CONTROLLER’S OR PROCESSOR’S ABILITY TO:

(I) COMPLY WITH FEDERAL, STATE, OR LOCAL LAWS, RULES, OR
REGULATIONS;

(II) COMPLY WITH A CIVIL, CRIMINAL, OR REGULATORY INQUIRY,
INVESTIGATION, SUBPOENA, OR SUMMONS BY FEDERAL, STATE, LOCAL, OR
OTHER GOVERNMENTAL AUTHORITIES;

(III) COOPERATE WITH LAW ENFORCEMENT AGENCIES CONCERNING
CONDUCT OR ACTIVITY THAT THE CONTROLLER OR PROCESSOR
REASONABLY AND IN GOOD FAITH BELIEVES MAY VIOLATE FEDERAL,
STATE, OR LOCAL LAW;

(IV) INVESTIGATE, EXERCISE, PREPARE FOR, OR DEFEND LEGAL
CLAIMS;

(V) CONDUCT INTERNAL RESEARCH TO IMPROVE, REPAIR, OR
DEVELOP PRODUCTS, SERVICES, OR TECHNOLOGY;

(VI) IDENTIFY AND REPAIR TECHNICAL ERRORS THAT IMPAIR
EXISTING OR INTENDED FUNCTIONALITY;

(VII) PERFORM INTERNAL OPERATIONS THAT ARE REASONABLY
ALIGNED WITH THE EXPECTATIONS OF THE CONSUMER BASED ON THE
CONSUMER’S EXISTING RELATIONSHIP WITH THE CONTROLLER;

(VIII) PROVIDE A PRODUCT OR SERVICE SPECIFICALLY REQUESTED
BY A CONSUMER, PERFORM A CONTRACT TO WHICH THE CONSUMER IS A
PARTY, OR TAKE STEPS AT THE REQUEST OF THE CONSUMER PRIOR TO
ENTERING INTO A CONTRACT;

(IX) PROTECT THE VITAL INTERESTS OF THE CONSUMER OR OF
ANOTHER INDIVIDUAL;

(X) PREVENT, DETECT, PROTECT AGAINST, OR RESPOND TO
SECURITY INCIDENTS, IDENTITY THEFT, FRAUD, HARASSMENT, OR MALICIOUS, DECEPTIVE, OR ILLEGAL ACTIVITY; PRESERVE THE INTEGRITY OR SECURITY OF SYSTEMS; OR INVESTIGATE, REPORT, OR PROSECUTE THOSE RESPONSIBLE FOR ANY SUCH ACTION:

(XI) PROCESS PERSONAL DATA FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, BUT SOLELY TO THE EXTENT THAT THE PROCESSING:

(A) IS SUBJECT TO SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS OF THE CONSUMER WHOSE PERSONAL DATA ARE PROCESSED; AND

(B) IS UNDER THE RESPONSIBILITY OF A PROFESSIONAL SUBJECT TO CONFIDENTIALITY OBLIGATIONS UNDER FEDERAL, STATE, OR LOCAL LAW; OR

(XII) ASSIST ANOTHER PERSON WITH ANY OF THE ACTIVITIES SET FORTH IN THIS SUBSECTION (3):

(b) APPLY WHERE COMPLIANCE BY THE CONTROLLER OR PROCESSOR WITH THIS PART 13 WOULD VIOLATE AN EVIDENTIARY PRIVILEGE UNDER COLORADO LAW;

(c) PREVENT A CONTROLLER OR PROCESSOR FROM PROVIDING PERSONAL DATA CONCERNING A CONSUMER TO A PERSON COVERED BY AN EVIDENTIARY PRIVILEGE UNDER COLORADO LAW AS PART OF A PRIVILEGED COMMUNICATION;

(d) APPLY TO INFORMATION MADE AVAILABLE BY A THIRD PARTY THAT THE CONTROLLER HAS A REASONABLE BASIS TO BELIEVE IS PROTECTED SPEECH PURSUANT TO APPLICABLE LAW; AND

(e) APPLY TO THE PROCESSING OF PERSONAL DATA BY AN INDIVIDUAL IN THE COURSE OF A PURELY PERSONAL OR HOUSEHOLD
ACTIVITY.

(4) PERSONAL DATA THAT ARE PROCESSED BY A CONTROLLER
PURSUANT TO AN EXCEPTION PROVIDED BY THIS SECTION:
(a) SHALL NOT BE PROCESSED FOR ANY PURPOSE OTHER THAN A
PURPOSE EXPRESSLY LISTED IN THIS SECTION OR AS OTHERWISE
AUTHORIZED BY THIS PART 13; AND
(b) SHALL BE PROCESSED SOLELY TO THE EXTENT THAT THE
PROCESSING IS NECESSARY, REASONABLE, AND PROPORTIONATE TO THE
SPECIFIC PURPOSE OR PURPOSES LISTED IN THIS SECTION OR AS OTHERWISE
AUTHORIZED BY THIS PART 13.

(5) IF A CONTROLLER PROCESSES PERSONAL DATA PURSUANT TO
AN EXEMPTION IN THIS SECTION, THE CONTROLLER BEARS THE BURDEN OF
DEMONSTRATING THAT THE PROCESSING QUALIFIES FOR THE EXEMPTION
AND COMPLIES WITH THE REQUIREMENTS IN SUBSECTION (4) OF THIS
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, INSO FAR 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:

(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.

6-1-1306. Consumer personal data rights - repeal.

(1) CONSUMERS MAY EXERCISE THE FOLLOWING RIGHTS BY SUBMITTING A REQUEST USING THE METHODS SPECIFIED BY THE CONTROLLER IN THE PRIVACY NOTICE REQUIRED UNDER SECTION 6-1-1308 (1)(a). THE METHOD MUST TAKE INTO ACCOUNT THE WAYS IN WHICH CONSUMERS NORMALLY INTERACT WITH THE CONTROLLER, THE NEED FOR SECURE AND RELIABLE COMMUNICATION RELATING TO THE REQUEST, AND THE ABILITY OF THE CONTROLLER TO AUTHENTICATE THE IDENTITY OF THE CONSUMER MAKING THE REQUEST. CONTROLLERS SHALL NOT REQUIRE A CONSUMER TO CREATE A NEW ACCOUNT IN ORDER TO EXERCISE CONSUMER RIGHTS PURSUANT TO THIS SECTION BUT MAY REQUIRE A CONSUMER TO USE AN EXISTING ACCOUNT. A CONSUMER MAY SUBMIT A REQUEST AT ANY TIME TO A CONTROLLER SPECIFYING WHICH OF THE FOLLOWING RIGHTS THE CONSUMER WISHES TO EXERCISE:

(a) Right to opt out. (I) A CONSUMER HAS THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR PURPOSES OF:

(A) TARGETED ADVERTISING;

(B) THE SALE OF PERSONAL DATA; OR

(C) PROFILING IN FURTHERANCE OF DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS CONCERNING A CONSUMER. 

(II) A CONSUMER MAY AUTHORIZE ANOTHER PERSON, ACTING ON THE CONSUMER'S BEHALF, TO OPT OUT OF THE PROCESSING OF THE CONSUMER'S PERSONAL DATA, INCLUDING THROUGH A TECHNOLOGY INDICATING THE CONSUMER'S INTENT TO OPT OUT SUCH AS A WEB LINK INDICATING A PREFERENCE OR BROWSER SETTING, BROWSER EXTENSION,
OR GLOBAL DEVICE SETTING, A CONTROLLER SHALL COMPLY WITH AN
OPT-OUT REQUEST RECEIVED FROM A PERSON AUTHORIZED BY THE
CONSUMER TO ACT ON THE CONSUMER'S BEHALF IF THE CONTROLLER IS
ABLE TO AUTHENTICATE, WITH COMMERCIAL REASONABLE EFFORT, THE
IDENTITY OF THE CONSUMER AND THE AUTHORIZED AGENT'S AUTHORITY
TO ACT ON THE CONSUMER'S BEHALF.

(III) A CONTROLLER THAT PROCESSES PERSONAL DATA FOR
PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA
SHALL PROVIDE A CLEAR AND CONSPICUOUS METHOD TO EXERCISE THE
RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING
THE CONSUMER PURSUANT TO SUBSECTION (I)(a)(I) OF THIS SECTION. THE
CONTROLLER SHALL PROVIDE THE OPT-OUT METHOD CLEARLY AND
CONSPICUOUSLY IN ANY PRIVACY NOTICE REQUIRED TO BE PROVIDED TO
CONSUMERS UNDER THIS PART 13, AND IN A CLEAR, CONSPICUOUS, AND
READILY ACCESSIBLE LOCATION OUTSIDE THE PRIVACY NOTICE.

(IV) (A) A CONTROLLER THAT PROCESSES PERSONAL DATA FOR
PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA
MAY ALLOW CONSUMERS TO EXERCISE THE RIGHT TO OPT OUT OF THE
PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR
PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA
PURSUANT TO SUBSECTIONS (I)(a)(I)(A) AND (I)(a)(I)(B) OF THIS SECTION
BY CONTROLLERS THROUGH A USER-SELECTED UNIVERSAL OPT-OUT
MECHANISM THAT MEETS THE TECHNICAL SPECIFICATIONS ESTABLISHED
BY THE ATTORNEY GENERAL PURSUANT TO SECTION 6-1-1313. THIS
SUBSECTION (I)(a)(IV)(A) IS REPEALED, EFFECTIVE JANUARY 1, 2024.

(B) EFFECTIVE JANUARY 1, 2024, A CONTROLLER THAT PROCESSES
PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE
OF PERSONAL DATA SHALL ALLOW CONSUMERS TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SUBSECTIONS (1)(a)(I)(A) AND (1)(a)(I)(B) OF THIS SECTION BY CONTROLLERS THROUGH A USER-SELECTED UNIVERSAL OPT-OUT MECHANISM THAT MEETS THE TECHNICAL SPECIFICATIONS ESTABLISHED BY THE ATTORNEY GENERAL PURSUANT TO SECTION 6-1-1313.

(C) NOTWITHSTANDING A CONSUMER'S DECISION TO EXERCISE THE RIGHT TO OPT OUT OF THE PROCESSING OF PERSONAL DATA THROUGH A UNIVERSAL OPT-OUT MECHANISM PURSUANT TO SUBSECTION (1)(a)(IV)(B) OF THIS SECTION, A CONTROLLER MAY ENABLE THE CONSUMER TO CONSENT, THROUGH A WEB PAGE, APPLICATION, OR A SIMILAR METHOD, TO THE PROCESSING OF THE CONSUMER'S PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA, AND THE CONSENT TAKES PRECEDENCE OVER ANY CHOICE REFLECTED THROUGH THE UNIVERSAL OPT-OUT MECHANISM. BEFORE OBTAINING A CONSUMER'S CONSENT TO PROCESS PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO THIS SUBSECTION (1)(a)(IV)(C), A CONTROLLER SHALL PROVIDE THE CONSUMER WITH A CLEAR AND CONSPICUOUS NOTICE INFORMING THE CONSUMER ABOUT THE CHOICES AVAILABLE UNDER THIS SECTION, DESCRIBING THE CATEGORIES OF PERSONAL DATA TO BE PROCESSED AND THE PURPOSES FOR WHICH THEY WILL BE PROCESSED, AND EXPLAINING HOW AND WHERE THE CONSUMER MAY WITHDRAW CONSENT. THE WEB PAGE, APPLICATION, OR OTHER MEANS BY WHICH A CONTROLLER OBTAINS A CONSUMER'S CONSENT TO PROCESS PERSONAL DATA FOR PURPOSES OF
TARGETED ADVERTISING OR THE SALE OF PERSONAL DATA MUST ALSO
ALLOW THE CONSUMER TO REVOKE THE CONSENT AS EASILY AS IT IS
AFFIRMATIVELY PROVIDED.

(b) **Right of access.** A CONSUMER HAS THE RIGHT TO CONFIRM
WHETHER A CONTROLLER IS PROCESSING PERSONAL DATA CONCERNING
THE CONSUMER AND TO ACCESS THE CONSUMER’S PERSONAL DATA.

(c) **Right to correction.** A CONSUMER HAS THE RIGHT TO CORRECT
INACCURACIES IN THE CONSUMER’S PERSONAL DATA, TAKING INTO
PROCESSING OF THE CONSUMER’S PERSONAL DATA.

(d) **Right to deletion.** A CONSUMER HAS THE RIGHT TO DELETE
PERSONAL DATA CONCERNING THE CONSUMER.

(e) **Right to data portability.** WHEN EXERCISING THE RIGHT TO
ACCESS PERSONAL DATA PURSUANT TO SUBSECTION (1)(b) OF THIS
SECTION, A CONSUMER HAS THE RIGHT TO OBTAIN THE PERSONAL DATA IN
A PORTABLE AND, TO THE EXTENT TECHNICALLY FEASIBLE, READILY
USABLE FORMAT THAT ALLOWS THE CONSUMER TO TRANSMIT THE DATA
TO ANOTHER ENTITY WITHOUT HINDRANCE. A CONSUMER MAY EXERCISE
THIS RIGHT NO MORE THAN TWO TIMES PER CALENDAR YEAR. NOTHING IN
THIS SUBSECTION (1)(e) REQUIRES A CONTROLLER TO PROVIDE THE DATA
TO THE CONSUMER IN A MANNER THAT WOULD DISCLOSE THE
CONTROLLER’S TRADE SECRETS.

(2) **Responding to consumer requests.** (a) A CONTROLLER
SHALL INFORM A CONSUMER OF ANY ACTION TAKEN ON A REQUEST UNDER
SUBSECTION (1) OF THIS SECTION WITHOUT UNDUE DELAY AND, IN ANY
EVENT, WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST. THE
CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY FORTY-FIVE
ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO
ACCOUNT THE COMPLEXITY AND NUMBER OF THE REQUESTS. THE
CONTROLLER SHALL INFORM THE CONSUMER OF AN EXTENSION WITHIN
FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST, TOGETHER WITH THE
REASONS FOR THE DELAY.

(b) If a controller does not take action on the request of
a consumer, the controller shall inform the consumer, without
undue delay and, at the latest, within forty-five days after
receipt of the request, of the reasons for not taking action and
instructions for how to appeal the decision with the controller
as described in subsection (3) of this section.

(c) Upon request, a controller shall provide to the
consumer the information specified in this section free of
charge; except that, for a second or subsequent request within
a twelve-month period, the controller may charge an amount
calculated in the manner specified in section 24-72-205 (5)(a).

(d) A controller is not required to comply with a request
to exercise any of the rights under subsection (1) of this section
if the controller is unable to authenticate the request using
commercially reasonable efforts, in which case the controller
may request the provision of additional information reasonably
necessary to authenticate the request.

(3) (a) A controller shall establish an internal process
whereby consumers may appeal a refusal to take action on a
request to exercise any of the rights under subsection (1) of this
section within a reasonable period after the consumer's receipt
of the notice sent by the controller under subsection (2)(b) of
THIS SECTION, THE APPEAL PROCESS MUST BE CONSPICUOUSLY AVAILABLE AND AS EASY TO USE AS THE PROCESS FOR SUBMITTING A REQUEST UNDER THIS SECTION.

(b) WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF AN APPEAL, A CONTROLLER SHALL INFORM THE CONSUMER OF ANY ACTION TAKEN OR NOT TAKEN IN RESPONSE TO THE APPEAL, ALONG WITH A WRITTEN EXPLANATION OF THE REASONS IN SUPPORT OF THE RESPONSE. THE CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY SIXTY ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO ACCOUNT THE COMPLEXITY AND NUMBER OF REQUESTS SERVING AS THE BASIS FOR THE APPEAL. THE CONTROLLER SHALL INFORM THE CONSUMER OF AN EXTENSION WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE APPEAL, TOGETHER WITH THE REASONS FOR THE DELAY.

(c) THE CONTROLLER SHALL INFORM THE CONSUMER OF THE CONSUMER'S ABILITY TO CONTACT THE ATTORNEY GENERAL IF THE CONSUMER HAS CONCERNS ABOUT THE RESULT OF THE APPEAL.

6-1-1307. Processing de-identified data. (1) THIS PART 13 DOES NOT REQUIRE A CONTROLLER OR PROCESSOR TO DO ANY OF THE FOLLOWING SOLELY FOR PURPOSES OF COMPLYING WITH THIS PART 13:

(a) REIDENTIFY DE-IDENTIFIED DATA;

(b) COMPLY WITH AN AUTHENTICATED CONSUMER REQUEST TO ACCESS, CORRECT, DELETE, OR PROVIDE PERSONAL DATA IN A PORTABLE FORMAT PURSUANT TO SECTION 6-1-1306 (1), IF ALL OF THE FOLLOWING ARE TRUE:

(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 USE THE PERSONAL DATA TO RECOGNIZE OR RESPOND TO THE SPECIFIC CONSUMER WHO IS THE SUBJECT OF THE PERSONAL DATA OR ASSOCIATE THE PERSONAL DATA WITH OTHER PERSONAL DATA ABOUT THE SAME SPECIFIC CONSUMER; AND

(III) THE CONTROLLER DOES NOT SELL THE PERSONAL DATA TO ANY THIRD PARTY OR OTHERWISE VOLUNTARILY DISCLOSE THE PERSONAL DATA TO ANY THIRD PARTY, EXCEPT AS OTHERWISE AUTHORIZED BY THE CONSUMER; OR

(c) MAINTAIN DATA IN IDENTIFIABLE FORM OR COLLECT, OBTAIN, RETAIN, OR ACCESS ANY DATA OR TECHNOLOGY IN ORDER TO ENABLE THE CONTROLLER TO ASSOCIATE AN AUTHENTICATED CONSUMER REQUEST WITH PERSONAL DATA.

(2) A CONTROLLER THAT USES DE-IDENTIFIED DATA SHALL EXERCISE REASONABLE OVERSIGHT TO MONITOR COMPLIANCE WITH ANY CONTRACTUAL COMMITMENTS TO WHICH THE DE-IDENTIFIED DATA ARE SUBJECT AND SHALL TAKE APPROPRIATE STEPS TO ADDRESS ANY BREACHES OF CONTRACTUAL COMMITMENTS.


(a) A CONTROLLER SHALL PROVIDE CONSUMERS WITH A REASONABLY ACCESSIBLE, CLEAR, AND MEANINGFUL PRIVACY NOTICE THAT INCLUDES:

(I) THE CATEGORIES OF PERSONAL DATA COLLECTED OR PROCESSED BY THE CONTROLLER OR A PROCESSOR;

(II) THE PURPOSES FOR WHICH THE CATEGORIES OF PERSONAL DATA ARE PROCESSED;

(III) HOW AND WHERE CONSUMERS MAY EXERCISE THE RIGHTS PURSUANT TO SECTION 6-1-1306, INCLUDING THE CONTROLLER’S CONTACT
INFORMATION AND HOW A CONSUMER MAY APPEAL A CONTROLLER’S
ACTION WITH REGARD TO THE CONSUMER’S REQUEST;

(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 PERSONAL DATA TO THIRD PARTIES OR
PROCESSES PERSONAL DATA FOR TARGETED ADVERTISING, THE
CONTROLLER SHALL CLEARLY AND CONSPICUOUSLY DISCLOSE THE SALE
OR PROCESSING, AS WELL AS THE MANNER IN WHICH A CONSUMER MAY
EXERCISE THE RIGHT TO OPT OUT OF THE SALE OR PROCESSING.

(c) A CONTROLLER SHALL NOT:

(I) REQUIRE A CONSUMER TO CREATE A NEW ACCOUNT IN ORDER
TO EXERCISE A RIGHT; OR

(II) BASED SOLELY ON THE EXERCISE OF A RIGHT AND UNRELATED
TO FEASIBILITY OR THE VALUE OF A SERVICE, INCREASE THE COST OF, OR
DECREASE THE AVAILABILITY OF, THE PRODUCT OR SERVICE.

(d) NOTHING IN THIS PART 13 SHALL BE CONSTRUED TO REQUIRE
A CONTROLLER TO PROVIDE A PRODUCT OR SERVICE THAT REQUIRES THE
PERSONAL DATA OF A CONSUMER THAT THE CONTROLLER DOES NOT
COLLECT OR MAINTAIN OR TO PROHIBIT A CONTROLLER FROM OFFERING A
DIFFERENT PRICE, RATE, LEVEL, QUALITY, OR SELECTION OF GOODS OR
SERVICES TO A CONSUMER, INCLUDING OFFERING GOODS OR SERVICES FOR
NO FEE, IF THE CONSUMER HAS EXERCISED THE RIGHT TO OPT OUT
PURSUANT TO THIS PART 13 OR THE OFFER IS RELATED TO A CONSUMER’S
VOLUNTARY PARTICIPATION IN A BONA FIDE LOYALTY, REWARDS,
PREMIUM FEATURES, DISCOUNT, OR CLUB CARD PROGRAM.
(2) **Duty of purpose specification.** A controller shall specify the express purposes for which personal data are collected and processed.

(3) **Duty of data minimization.** A controller's collection of personal data must be adequate, relevant, and limited to what is necessary in relation to the specified and express purposes for which the data are processed.

(4) **Duty to avoid secondary use.** A controller shall not process personal data for purposes that are not necessary to or compatible with the specified and express purposes for which the personal data are processed, unless the controller first obtains the consumer's consent.

(5) **Duty of care.** A controller shall take reasonable measures to secure personal data during both storage and use from unauthorized acquisition.

(6) **Duty to avoid unlawful discrimination.** A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

(7) **Duty regarding sensitive data.** A controller shall not process a consumer's sensitive data without first obtaining the consumer's consent or, in the case of the processing of personal data concerning a known child, without first obtaining consent from the child's parent or lawful guardian.

6-1-1309. **Data protection assessments - attorney general access and evaluation - definition.** (1) A controller shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data

-29- 190
PROTECTION ASSESSMENT OF EACH OF ITS PROCESSING ACTIVITIES THAT INVOLVE PERSONAL DATA ACQUIRED ON OR AFTER THE EFFECTIVE DATE OF THIS SECTION THAT PRESENT A HEIGHTENED RISK OF HARM TO A CONSUMER.

(2) FOR PURPOSES OF THIS SECTION, "PROCESSING THAT PRESENTS A HEIGHTENED RISK OF HARM TO A CONSUMER" INCLUDES THE FOLLOWING:

(a) PROCESSING PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING OR FOR PROFILING IF THE PROFILING PRESENTS A REASONABLY FORESEEABLE RISK OF:

(I) UNFAIR OR DECEPTIVE TREATMENT OF, OR UNLAWFUL DISPARATE IMPACT ON, CONSUMERS;

(II) FINANCIAL OR PHYSICAL INJURY TO CONSUMERS;

(III) A PHYSICAL OR OTHER INTRUSION UPON THE SOLITUDE OR SECLUSION, OR THE PRIVATE AFFAIRS OR CONCERNS, OF CONSUMERS IF THE INTRUSION WOULD BE OFFENSIVE TO A REASONABLE PERSON; OR

(IV) OTHER SUBSTANTIAL INJURY TO CONSUMERS;

(b) SELLING PERSONAL DATA; AND

(c) PROCESSING SENSITIVE DATA.

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.

(4) A CONTROLLER SHALL MAKE THE DATA PROTECTION
ASSESSMENT AVAILABLE TO THE ATTORNEY GENERAL UPON REQUEST. THE
ATTORNEY GENERAL MAY EVALUATE THE DATA PROTECTION ASSESSMENT
FOR COMPLIANCE WITH THE DUTIES CONTAINED IN SECTION 6-1-1308 AND
WITH OTHER LAWS, INCLUDING THIS ARTICLE 1. DATA PROTECTION
ASSESSMENTS ARE CONFIDENTIAL AND EXEMPT FROM PUBLIC INSPECTION
AND COPYING UNDER THE "COLORADO OPEN RECORDS ACT", PART 2 OF
ARTICLE 72 OF TITLE 24. THE DISCLOSURE OF A DATA PROTECTION
ASSESSMENT PURSUANT TO A REQUEST FROM THE ATTORNEY GENERAL
UNDER THIS SUBSECTION (4) DOES NOT CONSTITUTE A WAIVER OF ANY
ATTORNEY-CLIENT PRIVILEGE OR WORK-PRODUCT PROTECTION THAT
MIGHT OTHERWISE EXIST WITH RESPECT TO THE ASSESSMENT AND ANY
INFORMATION CONTAINED IN THE ASSESSMENT.

(5) A SINGLE DATA PROTECTION ASSESSMENT MAY ADDRESS A
COMPARABLE SET OF PROCESSING OPERATIONS THAT INCLUDE SIMILAR
ACTIVITIES.

(6) DATA PROTECTION ASSESSMENT REQUIREMENTS APPLY TO
PROCESSING ACTIVITIES CREATED OR GENERATED AFTER JULY 1, 2023,
AND ARE NOT RETROACTIVE.

6-1-1310. Liability. (1) NOTWITHSTANDING ANY PROVISION IN
PART 1 OF THIS ARTICLE 1, THIS PART 13 DOES NOT AUTHORIZE A PRIVATE
RIGHT OF ACTION FOR A VIOLATION OF THIS PART 13 OR ANY OTHER
PROVISION OF LAW. THIS SUBSECTION (1) NEITHER RELIEVES ANY PARTY
FROM ANY DUTIES OR OBLIGATIONS IMPOSED, NOR ALTERS ANY
INDEPENDENT RIGHTS THAT CONSUMERS HAVE, UNDER OTHER LAWS, INCLUDING THIS ARTICLE 1, THE STATE CONSTITUTION, OR THE UNITED STATES CONSTITUTION.

(2) WHERE MORE THAN ONE CONTROLLER OR PROCESSOR, OR BOTH A CONTROLLER AND A PROCESSOR, INVOLVED IN THE SAME PROCESSING VIOLATES THIS PART 13, THE LIABILITY SHALL BE ALLOCATED AMONG THE PARTIES ACCORDING TO PRINCIPLES OF COMPARATIVE FAULT.

6-1-1311. Enforcement - penalties - repeal.

(1)(a) NOTWITHSTANDING ANY OTHER PROVISION OF THIS ARTICLE 1, THE ATTORNEY GENERAL AND DISTRICT ATTORNEYS HAVE EXCLUSIVE AUTHORITY TO ENFORCE THIS PART 13 BY BRINGING AN ACTION IN THE NAME OF THE STATE OR AS PARENS PATRIAE ON BEHALF OF PERSONS RESIDING IN THE STATE TO ENFORCE THIS PART 13 AS PROVIDED IN THIS ARTICLE 1, INCLUDING SEEKING AN INJUNCTION TO ENJOIN A VIOLATION OF THIS PART 13.

(b) FOR PURPOSES ONLY OF ENFORCEMENT OF THIS PART 13 BY THE ATTORNEY GENERAL OR A DISTRICT ATTORNEY, A VIOLATION OF THIS PART 13 IS A DECEPTIVE TRADE PRACTICE.

(c) PRIOR TO ANY ENFORCEMENT ACTION PURSUANT TO SUBSECTION (1)(a) OF THIS SECTION, THE ATTORNEY GENERAL OR DISTRICT ATTORNEY MUST ISSUE A NOTICE OF VIOLATION TO THE CONTROLLER IF A CURE IS DEEMED POSSIBLE. IF THE CONTROLLER FAILS TO CURE THE VIOLATION WITHIN SIXTY DAYS AFTER RECEIPT OF THE NOTICE OF VIOLATION, AN ACTION MAY BE BROUGHT PURSUANT TO THIS SECTION. THIS SUBSECTION (1)(c) IS REPEALED, EFFECTIVE JANUARY 1, 2025.

(2) THE STATE TREASURER SHALL CREDIT ALL RECEIPTS FROM THE IMPOSITION OF CIVIL PENALTIES UNDER THIS PART 13 PURSUANT TO
SECTION 24-31-108.

6-1-1312. Preemption - local governments. This part 13 supercedes and preempts laws, ordinances, resolutions, regulations, or the equivalent adopted by any statutory or home rule municipality, county, or city and county regarding the processing of personal data by controllers or processors.

6-1-1313. Rules - opt-out mechanism. (1) The attorney general may promulgate rules for the purpose of carrying out this part 13.

(2) By December 31, 2023, the attorney general may adopt rules that detail the technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data pursuant to section 6-1-1306 (1)(a)(I)(A) or (1)(a)(I)(B). The attorney general shall update the rules that detail the technical specifications for the mechanisms from time to time to reflect the means by which consumers interact with controllers. The rules must:

(a) Not permit the manufacturer of a platform, browser, device, or any other product offering a universal opt-out mechanism to unfairly disadvantage another controller;
(b) Require controllers to inform consumers about the opt-out choices available under section 6-1-1306 (1)(a)(I);
(c) Not adopt a mechanism that is a default setting, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of
PERSONAL DATA PURSUANT TO SECTION 6-1-1306 (1)(a)(I)(A) OR
(1)(a)(I)(B):

(d) ADOPT A MECHANISM THAT IS CONSUMER-FRIENDLY, CLEARLY
DESCRIBED, AND EASY TO USE BY THE AVERAGE CONSUMER;

(e) ADOPT A MECHANISM THAT IS AS CONSISTENT AS POSSIBLE
WITH ANY OTHER SIMILAR MECHANISM REQUIRED BY LAW OR REGULATION
IN THE UNITED STATES; AND

(f) PERMIT THE CONTROLLER TO ACCURATELY AUTHENTICATE THE
CONSUMER AS A RESIDENT OF THIS STATE AND DETERMINE THAT THE
MECHANISM REPRESENTS A LEGITIMATE REQUEST TO OPT OUT OF THE
PROCESSING OF PERSONAL DATA FOR PURPOSES OF TARGETED
ADVERTISING OR THE SALE OF PERSONAL DATA PURSUANT TO SECTION

SECTION 2. In Colorado Revised Statutes, amend 6-1-104 as
follows:

6-1-104. Cooperative reporting. The district attorneys may
cooperate in a statewide reporting system by receiving, on forms provided
by the attorney general, complaints from persons concerning deceptive
trade practices listed in section 6-1-105 and OR part 7 OR 13 of this article
ARTICLE 1 and transmitting such THE complaints to the attorney general.

SECTION 3. In Colorado Revised Statutes, 6-1-105, add
(1)(nnn) as follows:

6-1-105. Unfair or deceptive trade practices. (1) A person
engages in a deceptive trade practice when, in the course of the person's
business, vocation, or occupation, the person;

(nnn) VIOLATES ANY PROVISION OF PART 13 OF THIS ARTICLE 1 AS
SPECIFIED IN SECTION 6-1-1311 (1)(b).
SECTION 4. In Colorado Revised Statutes, 6-1-107, amend (1)
introductory portion as follows:

6-1-107. Powers of attorney general and district attorneys.
(1) When the attorney general or a district attorney has reasonable cause
to believe that any person, whether in this state or elsewhere, has engaged
in or is engaging in any deceptive trade practice listed in section 6-1-105
or part 7 OR 13 of this article ARTICLE 1, the attorney general or district
attorney may:

SECTION 5. In Colorado Revised Statutes, 6-1-108, amend (1)
as follows:

6-1-108. Subpoenas - hearings - rules. (1) When the attorney
general or a district attorney has reasonable cause to believe that a person,
whether in this state or elsewhere, has engaged in or is engaging in a
deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this
article 1, the attorney general or a district attorney, in addition to other
powers conferred upon him or her THE ATTORNEY GENERAL OR A DISTRICT
ATTORNEY by this article 1, may issue subpoenas to require the attendance
of witnesses or the production of documents, administer oaths, conduct
hearings in aid of any investigation or inquiry, and prescribe such forms
and promulgate such rules as may be necessary to administer the
provisions of this article 1.

SECTION 6. In Colorado Revised Statutes, 6-1-110, amend (1)
and (2) as follows:

6-1-110. Restraining orders - injunctions - assurances of
discontinuance. (1) Whenever the attorney general or a district attorney
has cause to believe that a person has engaged in or is engaging in any
deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this
ARTICLE 1, the attorney general or district attorney may apply for and obtain, in an action in the appropriate district court of this state, a temporary restraining order or injunction, or both, pursuant to the Colorado rules of civil procedure, prohibiting such the person from continuing such the practices, or engaging therein, or doing any act in furtherance thereof. The court may make such orders or judgments as may be necessary to prevent the use or employment by such the person of any such deceptive trade practice or which that may be necessary to completely compensate or restore to the original position of any person injured by means of any such practice or to prevent any unjust enrichment by any person through the use or employment of any deceptive trade practice.

(2) Where the attorney general or a district attorney has authority to institute a civil action or other proceeding pursuant to the provisions of this article ARTICLE 1, the attorney general or district attorney may accept, in lieu thereof or as a part thereof, an assurance of discontinuance of any deceptive trade practice listed in section 6-1-105 or part 7 OR 13 of this article. Such the assurance may include a stipulation for the voluntary payment by the alleged violator of the costs of investigation and any action or proceeding by the attorney general or a district attorney and any amount necessary to restore to any person any money or property that may have been acquired by such the alleged violator by means of any such deceptive trade practice. Any such assurance of discontinuance accepted by the attorney general or a district attorney and any such stipulation filed with the court as a part of any such action or proceeding shall be a matter of public record unless the attorney general or the district attorney determines, at his or her discretion of the attorney
GENERAL OR DISTRICT ATTORNEY, that it will be confidential to the parties to the action or proceeding and to the court and its employees. Upon the filing of a civil action by the attorney general or a district attorney alleging that a confidential assurance of discontinuance or stipulation accepted pursuant to this subsection (2) has been violated, said THE assurance of discontinuance or stipulation shall thereupon be deemed BECOMES a public record and open to inspection by any person. Proof by a preponderance of the evidence of a violation of any such assurance or stipulation shall constitute CONSTITUTES prima facie evidence of a deceptive trade practice for the purposes of any civil action or proceeding brought thereafter by the attorney general or a district attorney, whether a new action or a subsequent motion or petition in any pending action or proceeding.

SECTION 7. Act subject to petition - effective date - applicability. (1) This act takes effect July 1, 2023; except that, if a referendum petition is filed pursuant to section 1 (3) of article V of the state constitution against this act or an item, section, or part of this act within the ninety-day period after final adjournment of the general assembly, then the act, item, section, or part will not take effect unless approved by the people at the general election to be held in November 2022 and, in such case, will take effect July 1, 2023, or on the date of the official declaration of the vote thereon by the governor, whichever is later.

(2) This act applies to conduct occurring on or after the applicable effective date of this act.