## First Regular Session Seventy-third General Assembly STATE OF COLORADO

## PREAMENDED

This Unofficial Version Includes Committee Amendments Not Yet Adopted on Second Reading

LLS NO. 21-0077.01 Thomas Morris x4218

SENATE BILL 21-190

SENATE SPONSORSHIP

Rodriguez and Lundeen,

(None),

## HOUSE SPONSORSHIP

Senate Committees Business, Labor, & Technology Appropriations **House Committees** 

# A BILL FOR AN ACT

#### 101 CONCERNING ADDITIONAL PROTECTION OF DATA RELATING TO

102 **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 <u>http://leg.colorado.gov.</u>)

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.

1	Be it enacted by the General Assembly of the State of Colorado:
2	SECTION 1. In Colorado Revised Statutes, add part 13 to article
3	1 of title 6 as follows:
4	PART 13
5	COLORADO PRIVACY ACT
6	<b>6-1-1301.</b> Short title. The short title of this part 13 is the
7	"COLORADO PRIVACY ACT".
8	6-1-1302. Legislative declaration. (1) THE GENERAL ASSEMBLY
9	HEREBY:
10	(a) FINDS THAT:
11	(I) The people of Colorado regard their privacy as a
12	FUNDAMENTAL RIGHT AND AN ESSENTIAL ELEMENT OF THEIR INDIVIDUAL

1 FREEDOM;

2 (II) COLORADO'S CONSTITUTION EXPLICITLY PROVIDES THE RIGHT
3 TO PRIVACY UNDER SECTION 7 OF ARTICLE II, AND FUNDAMENTAL PRIVACY
4 RIGHTS HAVE LONG BEEN, AND CONTINUE TO BE, INTEGRAL TO
5 PROTECTING COLORADANS AND TO SAFEGUARDING OUR DEMOCRATIC
6 REPUBLIC;

7 (III) ONGOING ADVANCES IN TECHNOLOGY HAVE PRODUCED
8 EXPONENTIAL GROWTH IN THE VOLUME AND VARIETY OF PERSONAL DATA
9 BEING GENERATED, COLLECTED, STORED, AND ANALYZED AND THESE
10 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;

21

(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;

26 (II) THE EUROPEAN UNION'S GENERAL DATA PROTECTION
27 REGULATION IS EMERGING AS A MODEL FOR COUNTRIES ACROSS THE

-3-

1 GLOBE IN DATA PRIVACY; AND

2 (III) STATES ACROSS THE UNITED STATES ARE LOOKING TO THIS
3 AND SIMILAR MODELS TO ENACT STATE-BASED DATA PRIVACY
4 REQUIREMENTS AND TO EXERCISE THE LEADERSHIP THAT IS LACKING AT
5 THE NATIONAL LEVEL; AND

6

(c) DECLARES THAT:

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

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

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

17 (B) IMPOSES AN AFFIRMATIVE OBLIGATION UPON COMPANIES TO
18 SAFEGUARD PERSONAL DATA; TO PROVIDE CLEAR, UNDERSTANDABLE, AND
19 TRANSPARENT INFORMATION TO CONSUMERS ABOUT HOW THEIR PERSONAL
20 DATA ARE USED; AND TO STRENGTHEN COMPLIANCE AND ACCOUNTABILITY
21 BY REQUIRING DATA PROTECTION ASSESSMENTS IN THE COLLECTION AND
22 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.

27 **6-1-1303. Definitions.** As used in this part 13, unless the

-4-

1 CONTEXT OTHERWISE REQUIRES:

2 (1) "AFFILIATE" MEANS A LEGAL ENTITY THAT CONTROLS, IS
3 CONTROLLED BY, OR IS UNDER COMMON CONTROL WITH ANOTHER LEGAL
4 ENTITY. AS USED IN THIS SUBSECTION (1), "CONTROL" MEANS:

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

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

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

16 (2) "AUTHENTICATE" MEANS TO USE REASONABLE MEANS TO
17 DETERMINE THAT A REQUEST TO EXERCISE ANY OF THE RIGHTS IN SECTION
18 6-1-1306 (1) IS BEING MADE BY OR ON BEHALF OF THE CONSUMER WHO IS
19 ENTITLED TO EXERCISE THE RIGHTS.

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

22 (4) "CHILD" MEANS AN INDIVIDUAL UNDER THIRTEEN YEARS OF23 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.

-5-

(6) "CONSUMER":

1

2 (a) MEANS AN INDIVIDUAL WHO IS A COLORADO RESIDENT ACTING 3 ONLY IN AN INDIVIDUAL OR HOUSEHOLD CONTEXT; AND 4 (b) DOES NOT INCLUDE AN INDIVIDUAL ACTING IN A COMMERCIAL 5 OR EMPLOYMENT CONTEXT, AS A JOB APPLICANT, OR AS A BENEFICIARY OF 6 SOMEONE ACTING IN AN EMPLOYMENT CONTEXT. 7 (7) "CONTROLLER" MEANS A PERSON THAT, ALONE OR JOINTLY 8 WITH OTHERS, DETERMINES THE PURPOSES FOR AND MEANS OF PROCESSING 9 PERSONAL DATA. 10 (8) "COVERED ENTITY" HAS THE MEANING ESTABLISHED IN 45 CFR 11 160.103. 12 (9) "DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT 13 EFFECTS CONCERNING A CONSUMER" MEANS A DECISION BASED SOLELY ON 14 AUTOMATED PROCESSING MADE BY THE CONTROLLER THAT RESULTS IN 15 THE PROVISION OR DENIAL BY THE CONTROLLER OF FINANCIAL OR LENDING 16 SERVICES, HOUSING, INSURANCE, EDUCATION ENROLLMENT, CRIMINAL 17 JUSTICE, EMPLOYMENT OPPORTUNITIES, HEALTH CARE SERVICES, OR 18 ACCESS TO BASIC NECESSITIES SUCH AS FOOD AND WATER. 19 (10) "DE-IDENTIFIED DATA" MEANS DATA THAT DO NOT IDENTIFY 20 AN INDIVIDUAL AND WITH RESPECT TO WHICH THERE IS NO REASONABLE 21 BASIS TO BELIEVE THAT THE INFORMATION CAN BE USED TO IDENTIFY AN 22 INDIVIDUAL. 23 "HEALTH CARE FACILITY" MEANS ANY ENTITY THAT IS (11)24 LICENSED, CERTIFIED, OR OTHERWISE AUTHORIZED OR PERMITTED BY LAW 25 TO ADMINISTER MEDICAL TREATMENT IN THIS STATE. 26 "HEALTH CARE INFORMATION" MEANS INDIVIDUALLY (12)27 IDENTIFIABLE INFORMATION RELATING TO THE PAST, PRESENT, OR FUTURE

1 HEALTH STATUS OF AN INDIVIDUAL.

(13) "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.

7 (<u>14</u>) "HIPAA" MEANS THE FEDERAL "HEALTH INSURANCE
8 PORTABILITY AND ACCOUNTABILITY ACT OF 1996", AS AMENDED, 42
9 U.S.C. SECS. 1320d TO 1320d-9.

10 (<u>15</u>) "IDENTIFIED OR IDENTIFIABLE INDIVIDUAL" MEANS AN
11 INDIVIDUAL WHO CAN BE READILY IDENTIFIED, DIRECTLY OR INDIRECTLY,
12 IN PARTICULAR BY REFERENCE TO AN IDENTIFIER SUCH AS A NAME, AN
13 IDENTIFICATION NUMBER, SPECIFIC GEOLOCATION DATA, OR AN ONLINE
14 IDENTIFIER.

15 (<u>16</u>) "PERSONAL DATA":

16 (a) MEANS INFORMATION THAT IS LINKED OR REASONABLY
17 LINKABLE TO AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL; AND

(b) DOES NOT INCLUDE DE-IDENTIFIED DATA OR PUBLICLY
AVAILABLE INFORMATION. AS USED IN THIS SUBSECTION (16)(b),
"PUBLICLY AVAILABLE INFORMATION" MEANS INFORMATION THAT IS
LAWFULLY MADE AVAILABLE FROM FEDERAL, STATE, OR LOCAL
GOVERNMENT <u>RECORDS AND</u> INFORMATION THAT A CONTROLLER HAS A
REASONABLE BASIS TO BELIEVE THE CONSUMER HAS LAWFULLY MADE
<u>AVAILABLE TO THE GENERAL PUBLIC.</u>

25 (<u>17</u>) "PROCESS" OR "PROCESSING" MEANS THE COLLECTION, USE,
26 SALE, STORAGE, DISCLOSURE, ANALYSIS, DELETION, OR MODIFICATION OF
27 PERSONAL DATA AND INCLUDES THE ACTIONS OF A CONTROLLER

-7-

1 DIRECTING A PROCESSOR TO PROCESS PERSONAL DATA.

2 (<u>18</u>) "PROCESSOR" MEANS A PERSON THAT PROCESSES PERSONAL
3 DATA ON BEHALF OF A CONTROLLER.

4 (<u>19</u>) "PROFILING" MEANS ANY FORM OF AUTOMATED PROCESSING
5 OF PERSONAL DATA TO EVALUATE, ANALYZE, OR PREDICT PERSONAL
6 ASPECTS CONCERNING AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL'S
7 ECONOMIC SITUATION, HEALTH, PERSONAL PREFERENCES, INTERESTS,
8 RELIABILITY, BEHAVIOR, LOCATION, OR MOVEMENTS.

9 (20) "PROTECTED HEALTH INFORMATION" HAS THE MEANING 10 ESTABLISHED IN 45 CFR 160.103.

11 (21) "PSEUDONYMOUS DATA" MEANS PERSONAL DATA THAT CAN 12 NO LONGER BE ATTRIBUTED TO AN INDIVIDUAL WITHOUT THE USE OF 13 ADDITIONAL INFORMATION IF THE ADDITIONAL INFORMATION IS KEPT 14 SEPARATELY AND IS SUBJECT TO TECHNICAL AND ORGANIZATIONAL 15 MEASURES TO ENSURE THAT THE PERSONAL DATA ARE NOT ATTRIBUTED 16 TO AN INDIVIDUAL.

17 (<u>22</u>) (a) "SALE", "SELL", OR "SOLD" MEANS THE EXCHANGE OF
18 PERSONAL DATA FOR MONETARY OR OTHER <u>VALUABLE</u> CONSIDERATION BY
19 A CONTROLLER TO A THIRD PARTY FOR PURPOSES OF LICENSING OR
20 SELLING PERSONAL DATA AT THE THIRD PARTY'S DISCRETION TO
21 ADDITIONAL THIRD PARTIES.

22

(b) "SALE" DOES NOT INCLUDE THE FOLLOWING:

23 (I) THE DISCLOSURE OF PERSONAL DATA TO A PROCESSOR THAT
24 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 OR OTHERWISE IN A MANNER THAT IS CONSISTENT WITH

-8-

<u>CONSUMERS'</u> REASONABLE EXPECTATIONS CONSIDERING THE CONTEXT IN
 WHICH THE CONSUMER PROVIDED THE PERSONAL DATA TO THE
 CONTROLLER;

4 (III) THE DISCLOSURE OR TRANSFER OF PERSONAL DATA TO AN
5 AFFILIATE OF THE CONTROLLER; \_\_\_\_\_

6 (IV) THE DISCLOSURE OR TRANSFER TO A THIRD PARTY OF 7 PERSONAL DATA AS AN ASSET THAT IS PART OF A <u>PROPOSED OR ACTUAL</u> 8 MERGER, ACQUISITION, BANKRUPTCY, OR OTHER TRANSACTION IN WHICH 9 THE THIRD PARTY ASSUMES CONTROL OF ALL OR PART OF THE 10 CONTROLLER'S <u>ASSETS; OR</u>

11 (V) THE DISCLOSURE OF PERSONAL DATA:

12 (A) THAT A CONSUMER DIRECTS THE CONTROLLER TO DISCLOSE OR

13 INTENTIONALLY DISCLOSES BY USING THE CONTROLLER TO INTERACT WITH

14 <u>A THIRD PARTY; OR</u>

15 (B) INTENTIONALLY MADE AVAILABLE TO THE GENERAL PUBLIC
 16 VIA A CHANNEL OF MASS MEDIA AND DID NOT RESTRICT TO A SPECIFIC

- 17 <u>AUDIENCE.</u>
- 18 (23) "SENSITIVE DATA" MEANS:

19 (a) PERSONAL DATA REVEALING RACIAL OR ETHNIC ORIGIN,
20 RELIGIOUS BELIEFS, A MENTAL OR PHYSICAL HEALTH CONDITION OR
21 DIAGNOSIS, SEX LIFE OR SEXUAL ORIENTATION, OR CITIZENSHIP OR
22 CITIZENSHIP STATUS;

- 23 (b) GENETIC OR BIOMETRIC DATA THAT MAY BE PROCESSED FOR
  24 THE PURPOSE OF UNIQUELY IDENTIFYING AN INDIVIDUAL; OR
- 25 (c) THE PERSONAL DATA FROM A KNOWN CHILD.
- 26
- 27 (24) "TARGETED ADVERTISING":

1 (a) MEANS DISPLAYING TO A CONSUMER AN ADVERTISEMENT THAT 2 IS SELECTED BASED ON PERSONAL DATA OBTAINED OR INFERRED OVER 3 TIME FROM THE CONSUMER'S ACTIVITIES ACROSS NONAFFILIATED 4 WEBSITES, APPLICATIONS, OR ONLINE SERVICES TO PREDICT CONSUMER 5 PREFERENCES OR INTERESTS; AND 6 (b) DOES NOT INCLUDE: 7 (I) ADVERTISING TO A CONSUMER IN RESPONSE TO THE 8 CONSUMER'S REQUEST FOR INFORMATION OR FEEDBACK; 9 (II) ADVERTISEMENTS BASED ON ACTIVITIES WITHIN A 10 CONTROLLER'S OWN WEBSITES OR ONLINE APPLICATIONS; 11 (III) ADVERTISEMENTS BASED ON THE CONTEXT OF A CONSUMER'S 12 CURRENT SEARCH QUERY, VISIT TO A WEBSITE, OR ONLINE APPLICATION; 13 OR 14 (IV) PROCESSING PERSONAL DATA SOLELY FOR MEASURING OR 15 REPORTING ADVERTISING PERFORMANCE, REACH, OR FREQUENCY. 16 "THIRD PARTY" MEANS A PERSON, PUBLIC AUTHORITY, (25)17 AGENCY, OR BODY OTHER THAN A CONSUMER, CONTROLLER, PROCESSOR, 18 OR AFFILIATE OF THE PROCESSOR OR THE CONTROLLER. 19 **6-1-1304.** Applicability of part. (1) EXCEPT AS SPECIFIED IN 20 SUBSECTION (2) OF THIS SECTION, THIS PART 13 APPLIES TO A CONTROLLER 21 THAT: 22 (a) CONDUCTS BUSINESS IN COLORADO OR PRODUCES PRODUCTS 23 OR SERVICES THAT ARE INTENTIONALLY TARGETED TO RESIDENTS OF 24 COLORADO; AND 25 (b) SATISFIES ONE OR BOTH OF THE FOLLOWING THRESHOLDS: 26 (I) CONTROLS OR PROCESSES THE PERSONAL DATA OF ONE 27 HUNDRED THOUSAND CONSUMERS OR MORE DURING A CALENDAR YEAR;

1 OR

6

7

2 (II) DERIVES REVENUE OR RECEIVES A DISCOUNT ON THE PRICE OF
3 GOODS OR SERVICES FROM THE SALE OF PERSONAL DATA AND PROCESSES
4 OR CONTROLS THE PERSONAL DATA OF TWENTY-FIVE THOUSAND
5 CONSUMERS OR MORE.

(2) This part 13 does not apply to:

(a) **PROTECTED HEALTH INFORMATION**;

8 (b) HEALTH CARE INFORMATION FOR PURPOSES OF PATIENT ACCESS
9 TO MEDICAL RECORDS PURSUANT TO PART 8 OF ARTICLE 1 OF TITLE 25;

10 (c) PATIENT IDENTIFYING INFORMATION, AS DEFINED IN 42 CFR
11 2.11, FOR PURPOSES OF 42 CFR 2, ESTABLISHED PURSUANT TO 42 U.S.C.
12 SEC. 290dd-2;

13 (d) IDENTIFIABLE PRIVATE INFORMATION, AS DEFINED IN 45 CFR 14 46.102, FOR PURPOSES OF THE FEDERAL POLICY FOR THE PROTECTION OF 15 HUMAN SUBJECTS PURSUANT TO 45 CFR 46; IDENTIFIABLE PRIVATE 16 INFORMATION THAT IS OTHERWISE INFORMATION COLLECTED AS PART OF 17 HUMAN SUBJECTS RESEARCH PURSUANT TO THE GOOD CLINICAL PRACTICE 18 GUIDELINES ISSUED BY THE INTERNATIONAL COUNCIL FOR 19 HARMONISATION OF TECHNICAL REQUIREMENTS FOR PHARMACEUTICALS 20 FOR HUMAN USE OR THE PROTECTION OF HUMAN SUBJECTS UNDER 21 CFR 21 50 AND 56; OR PERSONAL DATA USED OR SHARED IN RESEARCH 22 CONDUCTED IN ACCORDANCE WITH ONE OF MORE OF THE CATEGORIES SET 23 FORTH IN THIS SUBSECTION (2)(d);

24 (e) INFORMATION AND DOCUMENTS CREATED FOR PURPOSES OF
25 HIPAA AND ITS IMPLEMENTING REGULATIONS;

26 (f) PATIENT SAFETY WORK PRODUCT, AS DEFINED IN 42 CFR 3.20,
27 FOR PURPOSES OF PATIENT SAFETY IMPROVEMENT PURSUANT TO 42 CFR

1 3, ESTABLISHED PURSUANT TO 42 U.S.C. SECS. 299b-21 TO 299b-26;

2 (g) INFORMATION THAT IS:

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

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

7 (h) INFORMATION MAINTAINED IN THE SAME MANNER AS 8 INFORMATION UNDER SUBSECTIONS (2)(a) TO (2)(g) OF THIS SECTION BY:

9 (I) A COVERED ENTITY OR BUSINESS ASSOCIATE;

10 (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;

13 (i) (I) EXCEPT AS PROVIDED IN SUBSECTION (2)(i)(II) OF THIS 14 SECTION, AN ACTIVITY INVOLVING THE COLLECTION, MAINTENANCE, 15 DISCLOSURE, SALE, COMMUNICATION, OR USE OF ANY PERSONAL DATA 16 BEARING ON A CONSUMER'S CREDITWORTHINESS, CREDIT STANDING, 17 CREDIT CAPACITY, CHARACTER, GENERAL REPUTATION, PERSONAL 18 CHARACTERISTICS, OR MODE OF LIVING BY A CONSUMER REPORTING 19 AGENCY AS DEFINED IN 15 U.S.C. SEC. 1681a (f); BY A FURNISHER OF 20 INFORMATION AS SET FORTH IN 15 U.S.C. SEC. 1681s-2 THAT PROVIDES 21 INFORMATION FOR USE IN A CONSUMER REPORT, AS DEFINED IN 15 U.S.C. 22 SEC. 1681a (d); OR BY A USER OF A CONSUMER REPORT AS SET FORTH IN 15 23 U.S.C. SEC. 1681b.

(II) THIS SUBSECTION (2)(i) APPLIES ONLY TO THE EXTENT THAT
THE ACTIVITY IS REGULATED BY THE FEDERAL "FAIR CREDIT REPORTING
ACT", 15 U.S.C. SEC. 1681 ET SEQ., AS AMENDED, AND THE PERSONAL
DATA ARE NOT COLLECTED, MAINTAINED, DISCLOSED, SOLD,

-12-

- 1 COMMUNICATED, OR USED EXCEPT AS AUTHORIZED BY THE FEDERAL "FAIR
- 2 CREDIT REPORTING ACT", AS AMENDED.
  - (j) PERSONAL DATA:

- 4 (I) COLLECTED AND MAINTAINED FOR PURPOSES OF ARTICLE 22 OF
  5 TITLE 10;
- 6 (II) COLLECTED, PROCESSED, SOLD, OR DISCLOSED PURSUANT TO 7 THE FEDERAL "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET 8 SEQ., AS AMENDED, AND IMPLEMENTING REGULATIONS, IF THE 9 COLLECTION, PROCESSING, SALE, OR DISCLOSURE IS IN COMPLIANCE WITH 10 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
- 19 (V) REGULATED BY THE FEDERAL "FAMILY EDUCATIONAL RIGHTS
  20 AND PRIVACY ACT OF 1974", 20 U.S.C. SEC. 1232g ET SEQ., AS AMENDED,
  21 AND ITS IMPLEMENTING REGULATIONS:
- 22 (k) DATA MAINTAINED FOR EMPLOYMENT RECORDS PURPOSES;
- 23 (1) AN AIR CARRIER AS DEFINED IN AND REGULATED UNDER 49
- 24 <u>U.S.C. SEC. 40101 ET. SEQ., AS AMENDED, AND 49 U.S.C. SEC. 41713, AS</u>
- 25 <u>AMENDED;</u>
- 26 (<u>m</u>) INFORMATION USED AND DISCLOSED IN COMPLIANCE WITH 45
- 27 CFR 164.512; OR

1 (n) A FINANCIAL INSTITUTION OR AN AFFILIATE OF A FINANCIAL 2 INSTITUTION AS DEFINED BY AND THAT IS SUBJECT TO THE FEDERAL 3 "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ., AS 4 AMENDED, AND IMPLEMENTING REGULATIONS, INCLUDING REGULATION 5 <u>P, 12 CFR 1016.</u> 6 (3) THE OBLIGATIONS IMPOSED ON CONTROLLERS OR PROCESSORS 7 UNDER THIS PART 13 DO NOT: 8 (a) RESTRICT A CONTROLLER'S OR PROCESSOR'S ABILITY TO: 9 (I) COMPLY WITH FEDERAL, STATE, OR LOCAL LAWS, RULES, OR 10 **REGULATIONS:** 11 (II) COMPLY WITH A CIVIL, CRIMINAL, OR REGULATORY INQUIRY, 12 INVESTIGATION, SUBPOENA, OR SUMMONS BY FEDERAL, STATE, LOCAL, OR 13 OTHER GOVERNMENTAL AUTHORITIES; 14 (III) COOPERATE WITH LAW ENFORCEMENT AGENCIES CONCERNING 15 CONDUCT OR ACTIVITY THAT THE CONTROLLER OR PROCESSOR 16 REASONABLY AND IN GOOD FAITH BELIEVES MAY VIOLATE FEDERAL, 17 STATE, OR LOCAL LAW; 18 (IV) INVESTIGATE, EXERCISE, PREPARE FOR, OR DEFEND LEGAL 19 CLAIMS; 20 (V) CONDUCT INTERNAL RESEARCH TO IMPROVE, REPAIR, OR 21 DEVELOP PRODUCTS, SERVICES, OR TECHNOLOGY; 22 (VI) IDENTIFY AND REPAIR TECHNICAL ERRORS THAT IMPAIR 23 EXISTING OR INTENDED FUNCTIONALITY; 24 (VII) PERFORM INTERNAL OPERATIONS THAT ARE REASONABLY 25 ALIGNED WITH THE EXPECTATIONS OF THE CONSUMER BASED ON THE 26 CONSUMER'S EXISTING RELATIONSHIP WITH THE CONTROLLER; 27 (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;

4 (IX) PROTECT THE VITAL INTERESTS OF THE CONSUMER OR OF 5 ANOTHER INDIVIDUAL;

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

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

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

17 (B) IS UNDER THE RESPONSIBILITY OF A PROFESSIONAL SUBJECT TO
18 CONFIDENTIALITY OBLIGATIONS UNDER FEDERAL, STATE, OR LOCAL LAW;
19 (XII) ASSIST ANOTHER PERSON WITH ANY OF THE ACTIVITIES SET
20 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;

1 (d) ADVERSELY AFFECT THE RIGHTS OR FREEDOMS OF ANY 2 PERSONS, SUCH AS EXERCISING THE RIGHT OF FREE SPEECH PURSUANT TO 3 THE FIRST AMENDMENT TO THE UNITED STATES CONSTITUTION, AND A 4 CONSUMER'S EXERCISE OF THE RIGHTS CONTAINED IN SECTION 6-1-1306 5 (1)(a) AND (1)(d) DO NOT REQUIRE THE DELETION OF INFORMATION THAT 6 A CONTROLLER HAS A REASONABLE BASIS TO BELIEVE IS LAWFULLY MADE 7 AVAILABLE TO THE GENERAL PUBLIC BY A PERSON OTHER THAN THE 8 CONSUMER IN THE VALID EXERCISE OF THE PERSON'S FIRST AMENDMENT 9 RIGHTS; AND

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

(4) (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 (4)(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.

26 (5) PERSONAL DATA THAT ARE PROCESSED BY A CONTROLLER
27 PURSUANT TO <u>AN EXCEPTION PROVIDED BY</u> THIS SECTION:

(a) SHALL NOT BE PROCESSED FOR ANY PURPOSE OTHER THAN <u>A</u>
 <u>PURPOSE EXPRESSLY LISTED IN THIS SECTION OR AS OTHERWISE</u>
 <u>AUTHORIZED BY THIS PART 13; AND</u>

4 (b) SHALL BE PROCESSED SOLELY TO THE EXTENT THAT THE
5 PROCESSING IS NECESSARY, REASONABLE, AND PROPORTIONATE TO THE
6 SPECIFIC PURPOSE OR PURPOSES LISTED IN THIS <u>SECTION OR AS OTHERWISE</u>
7 AUTHORIZED BY THIS PART 13.

8 (6) IF A CONTROLLER PROCESSES PERSONAL DATA PURSUANT TO 9 AN EXEMPTION IN THIS SECTION, THE CONTROLLER BEARS THE BURDEN OF 10 DEMONSTRATING THAT THE PROCESSING QUALIFIES FOR THE EXEMPTION 11 AND COMPLIES WITH THE REQUIREMENTS IN SUBSECTION (5) OF THIS 12 SECTION.

6-1-1305. Responsibility according to role. (1) A CONTROLLER
SHALL MEET THE OBLIGATIONS ESTABLISHED UNDER THIS PART 13. A
CONTROLLER DOES NOT AVOID AN OBLIGATION BY DELEGATING
PROCESSING TO A PROCESSOR.

17 (2) A PROCESSOR SHALL ADHERE TO THE INSTRUCTIONS OF THE
18 CONTROLLER AND ASSIST THE CONTROLLER TO MEET ITS OBLIGATIONS
19 UNDER THIS PART 13.

20 (3) PROCESSING BY A PROCESSOR MUST BE GOVERNED BY A
21 BINDING CONTRACT BETWEEN THE CONTROLLER AND THE PROCESSOR
22 THAT SETS OUT THE PROCESSING INSTRUCTIONS TO WHICH THE PROCESSOR
23 IS BOUND.

(4) 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.
6-1-1306. Consumer personal data rights. (1) CONSUMERS MAY

-17-

1	EXERCISE THE FOLLOWING RIGHTS BY SUBMITTING A <u>REQUEST USING THE</u>
2	METHODS SPECIFIED BY THE CONTROLLER IN THE PRIVACY NOTICE. THE
3	METHOD MUST TAKE INTO ACCOUNT THE WAYS IN WHICH CONSUMERS
4	NORMALLY INTERACT WITH THE CONTROLLER, THE NEED FOR SECURE AND
5	RELIABLE COMMUNICATION RELATING TO THE REQUEST, AND THE ABILITY
6	OF THE CONTROLLER TO AUTHENTICATE THE IDENTITY OF THE CONSUMER
7	MAKING THE REQUEST. CONTROLLERS SHALL NOT REQUIRE A CONSUMER
8	TO CREATE A NEW ACCOUNT IN ORDER TO EXERCISE CONSUMER RIGHTS
9	PURSUANT TO THIS SECTION BUT MAY REQUIRE A CONSUMER TO USE AN
10	EXISTING ACCOUNT. A REQUEST MAY BE SUBMITTED AT ANY TIME, TO A
11	CONTROLLER THAT SPECIFIES WHICH RIGHTS THE CONSUMER WISHES TO
12	EXERCISE:
13	(a) Right to opt out. (I) A consumer has the right to opt out
14	OF THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER FOR
15	PURPOSES OF:
16	(A) TARGETED ADVERTISING;
17	(B) THE SALE OF PERSONAL DATA; OR
18	(C) PROFILING IN FURTHERANCE OF SOLELY AUTOMATED
19	DECISIONS THAT PRODUCE LEGAL OR SIMILARLY SIGNIFICANT EFFECTS
20	CONCERNING A CONSUMER.
21	(II) A CONSUMER MAY AUTHORIZE ANOTHER PERSON, ACTING ON
22	THE CONSUMER'S BEHALF, TO OPT OUT OF THE PROCESSING OF THE
23	CONSUMER'S PERSONAL DATA FOR PURPOSES OF TARGETED ADVERTISING
24	OR THE SALE OF THE CONSUMER'S PERSONAL <u>DATA, INCLUDING THROUGH</u>
25	A TECHNOLOGY INDICATING THE CONSUMERS INTENT TO OPT OUT SUCH AS
26	A BROWSER SETTING, BROWSER EXTENSION, OR GLOBAL DEVICE SETTING.
27	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
 REASONABLE EFFORT, THE IDENTITY OF THE CONSUMER AND THE
 AUTHORIZED AGENT'S AUTHORITY TO ACT ON THE CONSUMER'S BEHALF.

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

8 (c) Right to correction. A CONSUMER HAS THE RIGHT TO CORRECT
 9 <u>INACCURACIES IN THE CONSUMER'S PERSONAL DATA, TAKING INTO</u>
 10 <u>ACCOUNT THE NATURE OF THE PERSONAL DATA AND THE PURPOSES OF THE</u>
 11 <u>PROCESSING OF THE CONSUMER'S PERSONAL DATA.</u>

12 (d) Right to deletion. A CONSUMER HAS THE RIGHT TO DELETE
13 PERSONAL DATA CONCERNING THE <u>CONSUMER PROVIDED TO THE</u>
14 <u>CONTROLLER.</u>

15 (e) **Right to data portability.** WHEN EXERCISING THE RIGHT TO 16 ACCESS PERSONAL DATA PURSUANT TO SUBSECTION (1)(b) OF THIS 17 SECTION, A CONSUMER HAS THE RIGHT TO OBTAIN THE PERSONAL DATA IN 18 A PORTABLE AND, TO THE EXTENT TECHNICALLY FEASIBLE, READILY 19 USABLE FORMAT THAT ALLOWS THE CONSUMER TO TRANSMIT THE DATA 20 TO ANOTHER ENTITY WITHOUT HINDRANCE. A CONSUMER MAY EXERCISE 21 THIS RIGHT NO MORE THAN TWO TIMES PER CALENDAR YEAR. NOTHING IN 22 THIS SUBSECTION (1)(e) REQUIRES A CONTROLLER TO PROVIDE THE DATA 23 TO THE CONSUMER IN A MANNER THAT WOULD DISCLOSE THE 24 CONTROLLER'S TRADE SECRETS. 25 \_ \_\_\_ 26 (2) **Responding to consumer requests.** (a) A CONTROLLER

27 SHALL INFORM A CONSUMER OF ANY ACTION TAKEN ON A REQUEST UNDER

-19-

1 SUBSECTION (1) OF THIS SECTION WITHOUT UNDUE DELAY AND, IN ANY 2 EVENT, WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST. THE 3 CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY FORTY-FIVE 4 ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO 5 ACCOUNT THE COMPLEXITY AND NUMBER OF THE REQUESTS. THE 6 CONTROLLER SHALL INFORM THE CONSUMER OF AN EXTENSION WITHIN 7 FORTY-FIVE DAYS AFTER RECEIPT OF THE REQUEST, TOGETHER WITH THE 8 REASONS FOR THE DELAY.

9 (b) IF A CONTROLLER DOES NOT TAKE ACTION ON THE REQUEST OF 10 A CONSUMER, THE CONTROLLER SHALL INFORM THE CONSUMER, WITHOUT 11 UNDUE DELAY AND, AT THE LATEST, WITHIN FORTY-FIVE DAYS AFTER 12 RECEIPT OF THE REQUEST, OF THE REASONS FOR NOT TAKING ACTION AND 13 INSTRUCTIONS FOR HOW TO APPEAL THE DECISION WITH THE CONTROLLER 14 AS DESCRIBED IN SUBSECTION (3) OF THIS SECTION.

15 (c) UPON REQUEST, A CONTROLLER SHALL PROVIDE TO THE
16 CONSUMER THE INFORMATION SPECIFIED IN THIS SECTION FREE OF
17 CHARGE; EXCEPT THAT, FOR A SECOND OR SUBSEQUENT REQUEST WITHIN
18 A TWELVE-MONTH PERIOD, THE CONTROLLER MAY CHARGE AN AMOUNT
19 CALCULATED IN THE MANNER SPECIFIED IN SECTION 24-72-205 (5)(a).

20 (d) A CONTROLLER IS NOT REQUIRED TO COMPLY WITH A REQUEST
21 TO EXERCISE ANY OF THE RIGHTS UNDER SUBSECTION (1) OF THIS SECTION
22 IF THE CONTROLLER IS UNABLE TO AUTHENTICATE THE REQUEST USING
23 COMMERCIALLY REASONABLE EFFORTS, IN WHICH CASE THE CONTROLLER
24 MAY REQUEST THE PROVISION OF ADDITIONAL INFORMATION REASONABLY
25 NECESSARY TO AUTHENTICATE THE REQUEST.

26 (3) (a) A CONTROLLER SHALL ESTABLISH AN INTERNAL PROCESS
 27 WHEREBY CONSUMERS MAY APPEAL A REFUSAL TO TAKE ACTION ON A

-20-

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.

7 (b) WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF AN APPEAL, A 8 CONTROLLER SHALL INFORM THE CONSUMER OF ANY ACTION TAKEN OR 9 NOT TAKEN IN RESPONSE TO THE APPEAL, ALONG WITH A WRITTEN 10 EXPLANATION OF THE REASONS IN SUPPORT OF THE RESPONSE. THE 11 CONTROLLER MAY EXTEND THE FORTY-FIVE-DAY PERIOD BY SIXTY 12 ADDITIONAL DAYS WHERE REASONABLY NECESSARY, TAKING INTO 13 ACCOUNT THE COMPLEXITY AND NUMBER OF REQUESTS SERVING AS THE 14 BASIS FOR THE APPEAL. THE CONTROLLER SHALL INFORM THE CONSUMER 15 OF AN EXTENSION WITHIN FORTY-FIVE DAYS AFTER RECEIPT OF THE 16 APPEAL, TOGETHER WITH THE REASONS FOR THE DELAY.

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

6-1-1307. Processing de-identified data or pseudonymous 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;

24

(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

1 ARE TRUE:

2 (I) (A) THE CONTROLLER IS NOT REASONABLY CAPABLE OF 3 ASSOCIATING THE REQUEST WITH THE PERSONAL DATA; OR

4 (B) IT WOULD BE UNREASONABLY BURDENSOME FOR THE 5 CONTROLLER TO ASSOCIATE THE REQUEST WITH THE PERSONAL DATA;

6 (II) THE CONTROLLER DOES NOT USE THE PERSONAL DATA TO
7 RECOGNIZE OR RESPOND TO THE SPECIFIC CONSUMER WHO IS THE SUBJECT
8 OF THE PERSONAL DATA OR ASSOCIATE THE PERSONAL DATA WITH OTHER
9 PERSONAL DATA ABOUT THE SAME SPECIFIC CONSUMER; AND

10 (III) THE CONTROLLER DOES NOT SELL THE PERSONAL DATA TO
11 ANY THIRD PARTY OR OTHERWISE VOLUNTARILY DISCLOSE THE PERSONAL
12 DATA TO ANY THIRD <u>PARTY</u>, EXCEPT AS OTHERWISE PERMITTED BY THIS
13 PART 13; OR

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

18 (2) THE RIGHTS CONTAINED IN SECTION 6-1-1306 (1) DO NOT
19 APPLY TO PSEUDONYMOUS DATA IF THE CONTROLLER CAN DEMONSTRATE
20 THAT THE INFORMATION NECESSARY TO IDENTIFY THE CONSUMER IS KEPT
21 SEPARATELY AND IS SUBJECT TO EFFECTIVE TECHNICAL AND
22 ORGANIZATIONAL CONTROLS THAT PREVENT THE CONTROLLER FROM
23 ACCESSING THE INFORMATION.

(3) A CONTROLLER THAT USES PSEUDONYMOUS DATA OR
DE-IDENTIFIED DATA SHALL EXERCISE REASONABLE OVERSIGHT TO
MONITOR COMPLIANCE WITH ANY CONTRACTUAL COMMITMENTS TO WHICH
THE PSEUDONYMOUS DATA OR DE-IDENTIFIED DATA ARE SUBJECT AND

-22-

SHALL TAKE APPROPRIATE STEPS TO ADDRESS ANY BREACHES OF
 CONTRACTUAL COMMITMENTS.

3 (4) A CONTROLLER MAY DETERMINE THAT DATA ARE
4 DE-IDENTIFIED ONLY IF:

5 (a) A PERSON WITH APPROPRIATE KNOWLEDGE OF AND EXPERIENCE
6 WITH GENERALLY ACCEPTED STATISTICAL AND SCIENTIFIC PRINCIPLES AND
7 METHODS FOR RENDERING INFORMATION NOT INDIVIDUALLY
8 IDENTIFIABLE:

9 (I) APPLYING THOSE PRINCIPLES AND METHODS, DETERMINES THAT 10 THE RISK IS VERY SMALL, AS DETERMINED UNDER 45 CFR 164.514, THAT 11 THE INFORMATION COULD BE USED, ALONE OR IN COMBINATION WITH 12 OTHER REASONABLY AVAILABLE INFORMATION, BY AN ANTICIPATED 13 RECIPIENT TO IDENTIFY AN INDIVIDUAL WHO IS A SUBJECT OF THE 14 INFORMATION; AND

15 (II) DOCUMENTS THE METHODS AND RESULTS OF THE ANALYSIS
16 THAT JUSTIFY THE DETERMINATION; OR

17 (b) (I) THE FOLLOWING IDENTIFIERS OF THE INDIVIDUAL OR OF
18 RELATIVES, EMPLOYERS, OR HOUSEHOLD MEMBERS OF THE INDIVIDUAL,
19 ARE REMOVED:

20 (A) NAMES;

(B) ALL GEOGRAPHIC SUBDIVISIONS SMALLER THAN A STATE,
INCLUDING STREET ADDRESS, CITY, COUNTY, PRECINCT, ZIP CODE, AND
THEIR EQUIVALENT GEOCODES, EXCEPT FOR THE INITIAL THREE DIGITS OF
A ZIP CODE IF, ACCORDING TO THE CURRENT PUBLICLY AVAILABLE DATA
FROM THE FEDERAL CENSUS BUREAU: THE GEOGRAPHIC UNIT FORMED BY
COMBINING ALL ZIP CODES WITH THE SAME THREE INITIAL DIGITS
CONTAINS MORE THAN TWENTY THOUSAND PEOPLE; AND THE INITIAL

-23-

1 THREE DIGITS OF A ZIP CODE FOR ALL SUCH GEOGRAPHIC UNITS 2 CONTAINING TWENTY THOUSAND OR FEWER PEOPLE IS CHANGED TO 000; 3 (C) ALL ELEMENTS OF DATES, EXCEPT THE YEAR, FOR DATES 4 DIRECTLY RELATED TO AN INDIVIDUAL, INCLUDING BIRTH DATE, 5 ADMISSION DATE, DISCHARGE DATE, AND DATE OF DEATH; AND ALL AGES 6 NINETY OR OLDER AND ALL ELEMENTS OF DATES, INCLUDING YEAR, 7 INDICATIVE OF THAT AGE; EXCEPT THAT THE AGES AND ELEMENTS MAY BE 8 AGGREGATED INTO A SINGLE CATEGORY OF AGE NINETY OR OLDER; 9 (D) TELEPHONE NUMBERS; 10 (E) FAX NUMBERS; 11 (F) E-MAIL ADDRESSES; 12 (G) SOCIAL SECURITY NUMBERS; 13 (H) MEDICAL RECORD NUMBERS; 14 (I) HEALTH PLAN BENEFICIARY NUMBERS; 15 (J) ACCOUNT NUMBERS; 16 (K) CERTIFICATE AND LICENSE NUMBERS; 17 (L) VEHICLE IDENTIFIERS AND SERIAL NUMBERS, INCLUDING 18 LICENSE PLATE NUMBERS; 19 (M) DEVICE IDENTIFIERS AND SERIAL NUMBERS; 20 (N) WEB UNIVERSAL RESOURCE LOCATORS; 21 (O) INTERNET PROTOCOL ADDRESS NUMBERS; 22 (P) BIOMETRIC IDENTIFIERS, INCLUDING FINGERPRINTS AND 23 VOICEPRINTS; 24 (Q) FULL FACE PHOTOGRAPHIC IMAGES AND ANY COMPARABLE 25 IMAGES; AND 26 (R) ANY OTHER UNIQUE IDENTIFYING NUMBER, CHARACTERISTIC, 27 OR CODE, EXCEPT AS PERMITTED BY SUBSECTION (4)(b)(I)(B) OR

-24-

1 (4)(b)(I)(C) OF THIS SECTION; AND

2 (II) THE CONTROLLER DOES NOT HAVE ACTUAL KNOWLEDGE THAT
3 THE INFORMATION COULD BE USED ALONE OR IN COMBINATION WITH
4 OTHER INFORMATION TO IDENTIFY AN INDIVIDUAL WHO IS A SUBJECT OF
5 THE INFORMATION.

6 6-1-1308. Duties of controllers. (1) Duty of transparency.
7 (a) A CONTROLLER SHALL PROVIDE CONSUMERS WITH A REASONABLY
8 ACCESSIBLE, CLEAR, AND MEANINGFUL PRIVACY NOTICE THAT INCLUDES:

9 (I) THE CATEGORIES OF PERSONAL DATA COLLECTED OR 10 PROCESSED BY THE CONTROLLER OR A PROCESSOR;

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

13

14 (III) How and where consumers may exercise the rights
15 PURSUANT TO SECTION 6-1-1306, INCLUDING THE CONTROLLER'S CONTACT
16 INFORMATION AND HOW A CONSUMER MAY APPEAL A CONTROLLER'S
17 ACTION WITH REGARD TO THE CONSUMER'S REQUEST;

18 (IV) THE CATEGORIES OF PERSONAL DATA THAT THE CONTROLLER
 19 SHARES WITH THIRD PARTIES, IF ANY; AND

20 (V) THE CATEGORIES OF THIRD PARTIES, IF ANY, WITH WHOM THE
 21 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.

27 (c) A CONTROLLER SHALL NOT:

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

3 (II) BASED SOLELY ON THE EXERCISE OF A <u>RIGHT AND UNRELATED</u>
4 <u>TO FEASIBILITY OR THE VALUE OF A SERVICE</u>, INCREASE THE COST OF, OR
5 DECREASE THE AVAILABILITY OF, THE PRODUCT OR SERVICE.

6 (d) NOTHING IN THIS PART 13 SHALL BE CONSTRUED TO REQUIRE 7 A CONTROLLER TO PROVIDE A PRODUCT OR SERVICE THAT REQUIRES THE 8 PERSONAL DATA OF A CONSUMER THAT THE CONTROLLER DOES NOT 9 COLLECT OR MAINTAIN OR TO PROHIBIT A CONTROLLER FROM OFFERING A 10 DIFFERENT PRICE, RATE, LEVEL, QUALITY, OR SELECTION OF GOODS OR 11 SERVICES TO A CONSUMER, INCLUDING OFFERING GOODS OR SERVICES FOR 12 NO FEE, IF THE CONSUMER HAS EXERCISED THE RIGHT TO OPT OUT 13 PURSUANT TO THIS PART 13 OR THE OFFER IS RELATED TO A CONSUMER'S 14 VOLUNTARY PARTICIPATION IN A BONA FIDE LOYALTY, REWARDS,

15 PREMIUM FEATURES, DISCOUNT, OR CLUB CARD PROGRAM.

16 (2) Duty of purpose specification. A CONTROLLER SHALL SPECIFY
17 THE EXPRESS PURPOSES FOR WHICH PERSONAL DATA IS COLLECTED AND
18 PROCESSED.

19 (3) Duty of data minimization. A CONTROLLER'S COLLECTION OF
20 PERSONAL DATA MUST BE ADEQUATE, RELEVANT, AND LIMITED TO WHAT
21 IS NECESSARY IN RELATION TO THE SPECIFIED AND EXPRESS PURPOSES FOR
22 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 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.

4 (6) Duty to avoid unlawful discrimination. A CONTROLLER
5 SHALL NOT PROCESS PERSONAL DATA IN VIOLATION OF STATE <u>OR</u> FEDERAL
6 LAWS THAT PROHIBIT UNLAWFUL DISCRIMINATION AGAINST CONSUMERS.

7 (7) Duty regarding sensitive data. A CONTROLLER SHALL NOT
8 PROCESS SENSITIVE DATA <u>IT COLLECTS FROM A CONSUMER WITHOUT THE</u>
9 <u>CONSUMER RECEIVING CLEAR NOTICE AND THE OPPORTUNITY TO OPT OUT</u>
10 <u>OF PROCESSING OF THE CONSUMER'S SENSITIVE PERSONAL INFORMATION</u>
11 OR, IN THE CASE OF THE PROCESSING OF PERSONAL DATA CONCERNING A
12 KNOWN <u>CHILD</u>, WITHOUT OBTAINING CONSENT FROM THE CHILD'S \_\_\_\_\_\_
13 PARENT OR LAWFUL GUARDIAN.

14 6-1-1309. Data protection assessments - attorney general 15 access and evaluation. (1) A CONTROLLER SHALL NOT CONDUCT 16 PROCESSING THAT PRESENTS A HEIGHTENED RISK OF HARM TO A 17 CONSUMER WITHOUT CONDUCTING AND DOCUMENTING A DATA 18 PROTECTION ASSESSMENT OF EACH OF ITS PROCESSING ACTIVITIES THAT 19 INVOLVE PERSONAL DATA ACQUIRED ON OR AFTER THE EFFECTIVE DATE 20 OF THIS SECTION THAT PRESENT A HEIGHTENED RISK OF HARM TO A 21 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 <u>FOR PROFILING IF THE PROFILING PRESENTS A</u>
REASONABLY FORESEEABLE RISK OF:

-27-

1	(I) UNFAIR OR DECEPTIVE TREATMENT OF, OR UNLAWFUL
2	DISPARATE IMPACT ON, CONSUMERS;
3	(II) FINANCIAL OR PHYSICAL INJURY TO CONSUMERS;
4	(III) A PHYSICAL OR OTHER INTRUSION UPON THE SOLITUDE OR
5	SECLUSION, OR THE PRIVATE AFFAIRS OR CONCERNS, OF CONSUMERS IF THE
6	INTRUSION WOULD BE OFFENSIVE TO A REASONABLE PERSON; OR
7	(IV) OTHER SUBSTANTIAL INJURY TO CONSUMERS;
8	(b) SELLING PERSONAL DATA; AND

9 (c) PROCESSING SENSITIVE DATA.

10 (3) DATA PROTECTION ASSESSMENTS MUST IDENTIFY AND WEIGH 11 THE BENEFITS THAT MAY FLOW, DIRECTLY AND INDIRECTLY, FROM THE 12 PROCESSING TO THE CONTROLLER, THE CONSUMER, OTHER 13 STAKEHOLDERS, AND THE PUBLIC AGAINST THE POTENTIAL RISKS TO THE 14 RIGHTS OF THE CONSUMER ASSOCIATED WITH THE PROCESSING, AS 15 MITIGATED BY SAFEGUARDS THAT THE CONTROLLER CAN EMPLOY TO 16 REDUCE THE RISKS. THE CONTROLLER SHALL FACTOR INTO THIS 17 ASSESSMENT THE USE OF DE-IDENTIFIED DATA AND THE REASONABLE 18 EXPECTATIONS OF CONSUMERS, AS WELL AS THE CONTEXT OF THE 19 PROCESSING AND THE RELATIONSHIP BETWEEN THE CONTROLLER AND THE 20 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 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.

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

9 (6) DATA PROTECTION ASSESSMENT REQUIREMENTS APPLY TO
 10 PROCESSING ACTIVITIES CREATED OR GENERATED AFTER JANUARY 1,
 11 2023, AND ARE NOT RETROACTIVE.

12 6-1-1310. Liability. (1) NOTWITHSTANDING ANY PROVISION IN 13 PART 1 OF THIS ARTICLE 1, THIS PART 13 DOES NOT AUTHORIZE A PRIVATE 14 RIGHT OF ACTION FOR A VIOLATION OF THIS PART 13 OR ANY OTHER 15 PROVISION OF LAW. THIS SUBSECTION (1) NEITHER RELIEVES ANY PARTY 16 FROM ANY DUTIES OR OBLIGATIONS IMPOSED, NOR ALTERS ANY 17 INDEPENDENT RIGHTS THAT CONSUMERS HAVE, UNDER OTHER LAWS, 18 INCLUDING THIS ARTICLE 1, THE STATE CONSTITUTION, OR THE UNITED 19 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, UNLESS THE
LIABILITY IS OTHERWISE ALLOCATED BY CONTRACT AMONG THE PARTIES.
6-1-1311. Enforcement. (1) NOTWITHSTANDING ANY OTHER

26 PROVISION OF THIS ARTICLE 1:

27

(a) THE ATTORNEY GENERAL AND DISTRICT ATTORNEYS HAVE

-29-

1 EXCLUSIVE AUTHORITY TO ENFORCE THIS PART 13 BY FIRST ISSUING A 2 NOTICE OF VIOLATION TO THE CONTROLLER AND, IF THE CONTROLLER DOES 3 NOT CURE THE VIOLATION WITHIN SIXTY DAYS AFTER RECEIPT OF THE 4 NOTICE, BRINGING AN ACTION IN THE NAME OF THE STATE OR AS PARENS 5 PATRIAE ON BEHALF OF PERSONS RESIDING IN THE STATE TO ENFORCE THIS 6 PART 13, INCLUDING SEEKING AN INJUNCTION TO ENJOIN A VIOLATION OF 7 THIS PART 13; AND 8 (b) A CONTROLLER OR PROCESSOR THAT VIOLATES THIS PART 13: 9 (I) IS SUBJECT TO A CIVIL PENALTY AS SPECIFIED IN SECTION 10 6-1-112: AND 11 (II) MAY BE ENJOINED FROM VIOLATING THIS PART 13. 12 (2) THE STATE TREASURER SHALL CREDIT ALL RECEIPTS FROM THE 13 IMPOSITION OF CIVIL PENALTIES UNDER THIS PART 13 PURSUANT TO 14 SECTION 24-31-108. 15 (3) NOTHING IN THIS PART 13 CREATES OR PROVIDES A BASIS FOR 16 <u>A PRIVATE RIGHT OF ACTION ARISING UNDER THIS PART 13 OR UNDER ANY</u> 17 OTHER LAW FOR A VIOLATION OF THIS PART 13. 18 6-1-1312. Preemption - local governments. THIS PART 13 19 SUPERSEDES AND PREEMPTS LAWS, ORDINANCES, RESOLUTIONS, 20 REGULATIONS, OR THE EQUIVALENT ADOPTED BY ANY STATUTORY OR 21 HOME RULE MUNICIPALITY, COUNTY, OR CITY AND COUNTY REGARDING 22 THE PROCESSING OF PERSONAL DATA BY CONTROLLERS OR PROCESSORS. 23 SECTION 2. Act subject to petition - effective date -24 **applicability.** (1) This act takes effect January 1, 2023; except that, if a 25 referendum petition is filed pursuant to section 1 (3) of article V of the 26 state constitution against this act or an item, section, or part of this act 27 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 January 1, 2023, or on the date of
 the official declaration of the vote thereon by the governor, whichever is
 later.

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