

REFERENCE TITLE: personal data; processing; security standards

**State of Arizona
House of Representatives
Fifty-fifth Legislature
First Regular Session
2021**

HB 2865

**Introduced by
Representatives DeGrazia: Powers Hannley**

AN ACT

AMENDING TITLE 18, CHAPTER 5, ARIZONA REVISED STATUTES, BY ADDING ARTICLE 5; RELATING TO PERSONAL DATA.

(TEXT OF BILL BEGINS ON NEXT PAGE)

Be it enacted by the Legislature of the State of Arizona:

Section 1. Title 18, chapter 5, Arizona Revised Statutes, is amended by adding article 5, to read:

ARTICLE 5. DATA AND SECURITY STANDARDS

18-571. Definitions

IN THIS ARTICLE, UNLESS THE CONTEXT OTHERWISE REQUIRES:

1. "COLLECT" MEANS RECEIVING AND TAKING, INCLUDING BY AUTOMATED MEANS, ANY OPERATION OR SET OF OPERATIONS TO OBTAIN PERSONAL DATA, INCLUDING PURCHASING, LEASING, ASSEMBLING, RECORDING, GATHERING, ACQUIRING OR PROCURING PERSONAL DATA.

2. "CONSENT" MEANS A CLEAR, AFFIRMATIVE ACT SIGNIFYING A SPECIFIC, INFORMED AND UNAMBIGUOUS INDICATION OF A CONSUMER'S AGREEMENT TO COLLECT OR PROCESS THE CONSUMER'S PERSONAL DATA, SUCH AS BY A WRITTEN STATEMENT OR OTHER CLEAR AFFIRMATIVE ACTION.

3. "CONSUMER":

(a) MEANS A NATURAL PERSON WHO IS A RESIDENT OF THIS STATE AND WHO IS ACTING ONLY IN AN INDIVIDUAL, NONCOMMERCIAL OR HOUSEHOLD CONTEXT.

(b) DOES NOT INCLUDE A NATURAL PERSON WHO IS ACTING IN A COMMERCIAL OR EMPLOYMENT CONTEXT.

4. "CONTROLLER" MEANS THE NATURAL OR LEGAL PERSON THAT, ALONE OR JOINTLY WITH OTHERS, DETERMINES THE PURPOSES AND MEANS OF PROCESSING PERSONAL DATA.

5. "DATA BROKER" MEANS A BUSINESS, OR A UNIT OR UNITS OF A BUSINESS, SEPARATELY OR TOGETHER, THAT KNOWINGLY COLLECTS AND SELLS OR LICENSES TO THIRD PARTIES THE PERSONAL INFORMATION OF A CONSUMER WITH WHOM THE BUSINESS DOES NOT HAVE A DIRECT RELATIONSHIP.

6. "DEIDENTIFIED DATA" MEANS:

(a) DATA THAT CANNOT BE LINKED TO A KNOWN NATURAL PERSON WITHOUT ADDITIONAL INFORMATION KEPT SEPARATELY.

(b) DATA THAT MEETS ALL OF THE FOLLOWING:

(i) HAS BEEN MODIFIED TO A DEGREE THAT THE RISK OF REIDENTIFICATION IS SMALL.

(ii) IS SUBJECT TO A PUBLIC COMMITMENT BY THE CONTROLLER NOT TO ATTEMPT TO REIDENTIFY THE DATA.

(iii) TO WHICH ONE OR MORE ENFORCEABLE CONTROLS HAVE BEEN APPLIED TO PREVENT REIDENTIFICATION. FOR THE PURPOSES OF THIS ITEM, "ENFORCEABLE CONTROLS" INCLUDES LEGAL, ADMINISTRATIVE, TECHNICAL OR CONTRACTUAL CONTROLS.

7. "DISCLOSE" MEANS TAKING ANY ACTION, WITH RESPECT TO PERSONAL DATA, INCLUDING BY AUTOMATED MEANS, TO SELL, SHARE, PROVIDE OR OTHERWISE TRANSFER PERSONAL DATA TO ANOTHER ENTITY OR PERSON OR THE GENERAL PUBLIC.

8. "IDENTIFIED OR IDENTIFIABLE NATURAL PERSON" MEANS A PERSON WHO CAN BE READILY IDENTIFIED, DIRECTLY OR INDIRECTLY.

9. "PERSONAL DATA" OR "PERSONAL INFORMATION":

(a) MEANS ANY INFORMATION THAT IS OR CAN REASONABLY BE LINKED TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON.

(b) INCLUDES SENSITIVE DATA.

(c) DOES NOT INCLUDE DEIDENTIFIED DATA OR PUBLICLY AVAILABLE INFORMATION.

10. "PROCESS" OR "PROCESSING" MEANS COLLECTING, USING, STORING, DISCLOSING, ANALYZING, DELETING OR MODIFYING PERSONAL DATA, INCLUDING BY AUTOMATED MEANS.

11. "PROCESSOR" MEANS A NATURAL OR LEGAL PERSON THAT PROCESSES PERSONAL DATA ON BEHALF OF THE CONTROLLER.

12. "PROFILING" MEANS ANY FORM OF AUTOMATED PROCESSING OF PERSONAL DATA CONSISTING OF USING PERSONAL DATA TO EVALUATE CERTAIN PERSONAL ASPECTS ABOUT A NATURAL PERSON, PARTICULARLY ANALYZING OR PREDICTING ASPECTS OF THAT NATURAL PERSON'S ECONOMIC SITUATION, HEALTH, PERSONAL PREFERENCES, INTERESTS, RELIABILITY, BEHAVIOR, LOCATION OR MOVEMENTS.

13. "RESTRICTION OF PROCESSING" MEANS MARKING STORED PERSONAL DATA WITH THE AIM OF LIMITING THE PROCESSING OF SUCH PERSONAL DATA IN THE FUTURE.

14. "SALE":

(a) MEANS THE EXCHANGE OF PERSONAL DATA FOR MONETARY CONSIDERATION BY THE CONTROLLER TO A THIRD PARTY, INCLUDING FOR THE PURPOSES OF LICENSING OR SELLING PERSONAL DATA AT THE THIRD PARTY'S DISCRETION TO ADDITIONAL THIRD PARTIES.

(b) DOES NOT INCLUDE DISCLOSING PERSONAL DATA TO EITHER OF THE FOLLOWING:

(i) A PROCESSOR THAT PROCESSES THE PERSONAL DATA ON BEHALF OF THE CONTROLLER.

(ii) A THIRD PARTY WITH WHOM THE CONSUMER HAS A DIRECT RELATIONSHIP FOR PURPOSES OF PROVIDING A PRODUCT OR SERVICE REQUESTED BY THE CONSUMER OR OTHERWISE IN A MANNER THAT IS CONSISTENT WITH THE CONSUMER'S REASONABLE EXPECTATIONS CONSIDERING THE CONTEXT IN WHICH THE CONSUMER PROVIDED THE PERSONAL DATA TO THE CONTROLLER.

15. "SENSITIVE DATA" MEANS:

(a) PERSONAL DATA THAT REVEALS A NATURAL PERSON'S RACIAL OR ETHNIC ORIGINS, RELIGIOUS BELIEFS, MENTAL, PHYSICAL, BEHAVIORAL OR PSYCHOLOGICAL HEALTH CONDITIONS OR DIAGNOSES OR SEX LIFE OR SEXUAL ORIENTATION.

(b) GENETIC OR BIOMETRIC DATA THAT IS PROCESSED TO UNIQUELY IDENTIFY A NATURAL PERSON.

(c) THE PRECISE GEOLOCATION INFORMATION OF A DEVICE ASSOCIATED WITH A NATURAL PERSON.

(d) THE PERSONAL DATA OF A KNOWN CHILD.

16. "TARGETED ADVERTISING":

(a) MEANS DISPLAYING TO A CONSUMER ADVERTISEMENTS THAT ARE SELECTED BASED ON PERSONAL DATA OBTAINED OR INFERRED OVER TIME FROM THE CONSUMER'S ACTIVITIES ACROSS NONAFFILIATED WEBSITES, APPLICATIONS OR ONLINE SERVICES TO PREDICT USER PREFERENCES OR INTERESTS.

(b) DOES NOT INCLUDE ADVERTISING TO A CONSUMER BASED ON THE CONSUMER'S VISITS TO A WEBSITE, APPLICATION OR ONLINE SERVICE THAT A REASONABLE CONSUMER WOULD BELIEVE TO BE ASSOCIATED WITH THE PUBLISHER IN WHICH THE ADVERTISING IS PLACED BASED ON COMMON BRANDING, TRADEMARKS OR OTHER INDICIA OF COMMON OWNERSHIP OR IN RESPONSE TO THE CONSUMER'S REQUEST FOR INFORMATION OR FEEDBACK.

17. "VERIFIED REQUEST" MEANS THE PROCESS THROUGH WHICH A CONSUMER MAY SUBMIT A REQUEST TO EXERCISE A RIGHT OR RIGHTS SET FORTH IN THIS ARTICLE AND BY WHICH A CONTROLLER CAN REASONABLY AUTHENTICATE THE REQUEST AND THE CONSUMER MAKING THE REQUEST USING COMMERCIALY REASONABLE MEANS.

18-572. Consumer rights; access to personal data; verified requests; controller's duty.

A. A CONTROLLER SHALL FACILITATE VERIFIED REQUESTS FROM CONSUMERS TO EXERCISE CONSUMER RIGHTS AS FOLLOWS:

1. ON RECEIPT OF A VERIFIED REQUEST FROM A CONSUMER, A CONTROLLER SHALL NOTIFY THE CONSUMER WHETHER PERSONAL DATA CONCERNING THE CONSUMER IS BEING PROCESSED, HELD OR SOLD TO DATA BROKERS. ♠ IF PERSONAL

DATA IS BEING SOLD TO DATA BROKERS, THE CONTROLLER SHALL NOTIFY THE CONSUMER OF THE TYPE AND CATEGORY OF PERSONAL DATA THAT HAS BEEN SOLD AND TO WHOM THE PERSONAL DATA HAS BEEN SOLD.

2. ON RECEIPT OF A VERIFIED REQUEST FOR DISCLOSURE FROM A CONSUMER, IF PERSONAL DATA CONCERNING THE CONSUMER IS BEING PROCESSED OR HELD BY THE CONTROLLER, THE CONTROLLER SHALL PROVIDE A COPY OF THE PERSONAL DATA THAT THE CONTROLLER PROCESSES OR MAINTAINS OR PROVIDE THE CATEGORY OR TYPE OF PERSONAL INFORMATION THAT IS KEPT IF A COPY IS UNAVAILABLE OR UNATTAINABLE. ♦ IF THE CONSUMER MAKES THE REQUEST BY ELECTRONIC MEANS, AND UNLESS REQUESTED BY THE CONSUMER, THE INFORMATION MUST BE PROVIDED IN A COMMONLY USED ELECTRONIC FORM. ♦ FOR ANY ADDITIONAL COPIES REQUESTED BY THE CONSUMER, THE CONTROLLER MAY CHARGE A REASONABLE FEE BASED ON ADMINISTRATIVE COSTS.

3. A CONTROLLER THAT COLLECTS A CONSUMER'S PERSONAL DATA, AT OR BEFORE THE POINT OF COLLECTION, SHALL INFORM THE CONSUMER OF THE CATEGORIES OF PERSONAL DATA TO BE COLLECTED AND THE PURPOSES FOR WHICH THE CATEGORIES OF PERSONAL DATA WILL BE USED. ♦ A CONTROLLER MAY NOT COLLECT ADDITIONAL CATEGORIES OF PERSONAL DATA OR USE PERSONAL DATA COLLECTED FOR ADDITIONAL PURPOSES WITHOUT PROVIDING THE CONSUMER WITH NOTICE CONSISTENT WITH THIS SECTION.

4. A CONTROLLER SHALL PROVIDE THE INFORMATION SPECIFIED IN THIS SUBSECTION TO A CONSUMER ONLY ON RECEIPT OF A VERIFIED REQUEST.

B. THIS SECTION DOES NOT REQUIRE A CONTROLLER TO:

1. RETAIN ANY PERSONAL DATA COLLECTED FOR A SINGLE, ONETIME TRANSACTION IF THE CONTROLLER DOES NOT SELL OR RETAIN THE INFORMATION.

2. REIDENTIFY OR OTHERWISE LINK ANY DATA THAT, IN THE ORDINARY COURSE OF THE CONTROLLER, IS NOT MAINTAINED IN A MANNER THAT WOULD BE CONSIDERED PERSONAL DATA.

C. A CONTROLLER IS PRESUMED TO HAVE SOLD PERSONAL DATA IF THERE IS AN EXCHANGE OF PERSONAL DATA AND IF CONTRACT TERMS WITH THE THIRD PARTY DO NOT LIMIT THE USE OF PERSONAL INFORMATION BY THE THIRD PARTY.

D. THIS SECTION DOES NOT ADVERSELY AFFECT THE RIGHTS OR FREEDOMS OF OTHERS.

18-573. Personal information; correction; deletion; verified requests; requirements; exceptions

A. ON RECEIPT OF A VERIFIED REQUEST FROM A CONSUMER, THE CONTROLLER, WITHOUT UNDUE DELAY, SHALL CORRECT INACCURATE PERSONAL DATA CONCERNING THE CONSUMER THAT THE CONTROLLER MAINTAINS IN IDENTIFIABLE FORM. TAKING INTO ACCOUNT THE BUSINESS PURPOSES OF THE PROCESSING, THE CONTROLLER SHALL COMPLETE INCOMPLETE PERSONAL DATA, INCLUDING BY MEANS OF PROVIDING A SUPPLEMENTARY STATEMENT IF APPROPRIATE. IF THE CONTROLLER NO LONGER HAS THE CONSUMER'S PERSONAL DATA, THE CONTROLLER SHALL NOTIFY THE CONSUMER THAT THE PERSONAL DATA NO LONGER EXISTS AND MAY ASK IF THE CONSUMER WOULD LIKE TO ADD THE CONSUMER'S PERSONAL INFORMATION.

B. A CONTROLLER THAT COLLECTS PERSONAL DATA ABOUT CONSUMERS SHALL DISCLOSE TO EACH CONSUMER THE RIGHT TO REQUEST THE DELETION OF THE CONSUMER'S PERSONAL DATA.

C. ON RECEIPT OF A VERIFIED REQUEST FOR DELETION FROM A CONSUMER, A CONTROLLER SHALL DELETE THE CONSUMER'S PERSONAL DATA WITHOUT UNDUE DELAY IF ONE OF THE FOLLOWING APPLIES:

1. THE PERSONAL DATA IS NO LONGER NECESSARY IN RELATION TO THE PURPOSES FOR WHICH THE PERSONAL DATA WAS COLLECTED OR OTHERWISE PROCESSED.

2. FOR PROCESSING THAT REQUIRES CONSENT, THE CONSUMER WITHDRAWS CONSENT TO PROCESSING AND THERE ARE NO BUSINESS PURPOSES FOR THE PROCESSING.

3. THE PERSONAL DATA MUST BE DELETED TO COMPLY WITH A LEGAL OBLIGATION UNDER A FEDERAL, STATE OR LOCAL LAW OR REGULATION TO WHICH THE CONTROLLER IS SUBJECT.

4. THE CONTROLLER IS REQUIRED TO CERTIFY WHEN THE DELETION WAS COMPLETED.

5. THE PERSONAL DATA HAS BEEN UNLAWFULLY PROCESSED.

D. A CONTROLLER OR PROCESSOR IS NOT REQUIRED TO COMPLY WITH A CONSUMER'S REQUEST TO DELETE THE CONSUMER'S PERSONAL DATA IF IT IS NECESSARY FOR THE CONTROLLER OR PROCESSOR TO MAINTAIN THE CONSUMER'S PERSONAL DATA IN ORDER TO COMPLETE THE TRANSACTION FOR WHICH THE PERSONAL DATA WAS COLLECTED, PROVIDE A GOOD OR SERVICE REQUESTED BY THE CONSUMER OR REASONABLY ANTICIPATED WITHIN THE CONTEXT OF A CONTROLLER'S ONGOING BUSINESS RELATIONSHIP WITH THE CONSUMER OR OTHERWISE PERFORM A CONTRACT BETWEEN THE CONTROLLER AND THE CONSUMER.

E. IF A CONTROLLER IS REQUIRED TO DELETE PERSONAL DATA THAT THE CONTROLLER MAINTAINS IN IDENTIFIABLE FORM THAT HAS BEEN DISCLOSED TO THIRD PARTIES BY THE CONTROLLER, INCLUDING DATA BROKERS THAT RECEIVED THE PERSONAL DATA THROUGH A SALE, THE CONTROLLER SHALL TAKE REASONABLE STEPS TO INFORM OTHER CONTROLLERS OF WHICH IT IS AWARE THAT ARE PROCESSING SUCH PERSONAL DATA AND THAT RECEIVED SUCH PERSONAL DATA FROM THE CONTROLLER OR ARE PROCESSING SUCH PERSONAL DATA ON BEHALF OF THE CONTROLLER THAT THE CONSUMER HAS REQUESTED THE DELETION BY THE OTHER CONTROLLERS OF ANY LINK TO OR COPY OR REPLICATION OF THE PERSONAL DATA. COMPLIANCE WITH THIS SUBSECTION MUST TAKE INTO ACCOUNT AVAILABLE TECHNOLOGY AND COST OF IMPLEMENTATION.

F. THIS SECTION DOES NOT APPLY TO THE EXTENT THAT PROCESSING IS NECESSARY:

1. FOR EXERCISING THE RIGHT OF FREE SPEECH.

2. FOR COMPLYING WITH A LEGAL OBLIGATION THAT REQUIRES PROCESSING OF PERSONAL DATA BY A FEDERAL, STATE OR LOCAL LAW OR REGULATION TO WHICH THE CONTROLLER IS SUBJECT OR FOR PERFORMING A TASK CARRIED OUT IN THE PUBLIC INTEREST OR IN EXERCISING OFFICIAL AUTHORITY VESTED IN THE CONTROLLER.

3. FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, IF THE PROCESSING IS BOTH OF THE FOLLOWING:

(a) SUBJECT TO SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS OF THE CONSUMER.

(b) UNDER THE RESPONSIBILITY OF A PROFESSIONAL SUBJECT TO CONFIDENTIALITY OBLIGATIONS UNDER A FEDERAL, STATE OR LOCAL LAW OR REGULATION.

4. FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES, IF DELETING SUCH PERSONAL DATA IS LIKELY TO RENDER IMPOSSIBLE OR SERIOUSLY IMPAIR THE ACHIEVEMENT OF THE OBJECTIVES OF THE PROCESSING.

5. FOR ESTABLISHING, EXERCISING OR DEFENDING LEGAL CLAIMS.

6. TO DETECT OR RESPOND TO SECURITY INCIDENTS, PROTECT AGAINST MALICIOUS, DECEPTIVE, FRAUDULENT OR ILLEGAL ACTIVITY OR IDENTIFY, INVESTIGATE OR PROSECUTE THOSE RESPONSIBLE FOR THAT ACTIVITY.

18-574. Restriction of processing; verified requests; requirements

A. ON RECEIPT OF A VERIFIED REQUEST FROM A CONSUMER, THE CONTROLLER SHALL RESTRICT PROCESSING OF PERSONAL DATA IF ANY OF THE

FOLLOWING APPLIES:

1. THE ACCURACY OF THE PERSONAL DATA IS CONTESTED BY THE CONSUMER, FOR A PERIOD ENABLING THE CONTROLLER TO VERIFY THE ACCURACY OF THE PERSONAL DATA.

2. THE PROCESSING IS UNLAWFUL AND THE CONSUMER OPPOSES THE DELETION OF THE PERSONAL DATA AND INSTEAD REQUESTS THE RESTRICTION OF PROCESSING.

3. THE CONTROLLER NO LONGER NEEDS THE PERSONAL DATA FOR THE PURPOSES OF THE PROCESSING BUT SUCH PERSONAL DATA IS REQUIRED BY THE CONSUMER FOR ESTABLISHING, EXERCISING OR DEFENDING LEGAL CLAIMS.

4. THE CONSUMER OBJECTS TO THE PROCESSING PENDING THE VERIFICATION OF WHETHER THE LEGITIMATE GROUNDS OF THE CONTROLLER OVERRIDE THOSE OF THE CONSUMER.

B. IF PERSONAL DATA IS SUBJECT TO A RESTRICTION OF PROCESSING UNDER THIS SECTION, THE PERSONAL DATA, EXCEPT FOR STORAGE, MAY BE PROCESSED ONLY AS FOLLOWS:

1. WITH THE CONSUMER'S CONSENT.

2. TO ESTABLISH, EXERCISE OR DEFEND LEGAL CLAIMS.

3. TO PROTECT THE RIGHTS OF ANOTHER NATURAL OR LEGAL PERSON.

4. FOR REASONS OF IMPORTANT PUBLIC INTEREST UNDER A FEDERAL, STATE OR LOCAL LAW OR REGULATION.

C. THE CONTROLLER SHALL INFORM A CONSUMER WHO HAS OBTAINED RESTRICTION OF PROCESSING PURSUANT TO THIS SECTION BEFORE THE RESTRICTION OF PROCESSING IS LIFTED AND THE PROPOSED LEGAL BASIS FOR DOING SO.

18-575. Receiving personal data; verified requests

A. ON A VERIFIED REQUEST FROM A CONSUMER, THE CONTROLLER SHALL PROVIDE TO THE CONSUMER, IF TECHNICALLY FEASIBLE AND COMMERCIALY REASONABLE, ANY PERSONAL DATA THAT THE CONTROLLER MAINTAINS IN IDENTIFIABLE FORM CONCERNING THE CONSUMER THAT THE CONSUMER HAS PROVIDED TO THE CONTROLLER IN A STRUCTURED, COMMONLY USED AND MACHINE-READABLE FORMAT:

1. IF PROCESSING THE PERSONAL DATA IS NECESSARY TO PERFORM A CONTRACT TO WHICH THE CONSUMER IS A PARTY.

2. IN ORDER TO TAKE STEPS AT THE REQUEST OF THE CONSUMER BEFORE ENTERING INTO A CONTRACT.

3. IF THE PROCESSING IS CARRIED OUT BY AUTOMATED MEANS.

B. REQUESTS FOR PERSONAL DATA UNDER THIS SECTION MUST BE WITHOUT PREJUDICE TO THE CONSUMER'S RIGHT TO DELETE.

C. THE RIGHTS PROVIDED IN THIS SECTION DO NOT APPLY TO PROCESSING NECESSARY TO PERFORM A TASK CARRIED OUT IN THE PUBLIC INTEREST OR TO EXERCISE OFFICIAL AUTHORITY VESTED IN THE CONTROLLER AND MUST NOT ADVERSELY AFFECT THE RIGHTS OF OTHERS.

18-576. Objection to processing of personal data

A. A CONSUMER MAY OBJECT, THROUGH A VERIFIED OBJECTION, AT ANY TIME, TO THE PROCESSING OF PERSONAL DATA CONCERNING THE CONSUMER.

B. ON RECEIPT OF A CONSUMER'S VERIFIED OBJECTION TO PROCESSING THE CONSUMER'S PERSONAL DATA FOR TARGETED ADVERTISING, WHICH INCLUDES THE SALE OF PERSONAL DATA THAT CONCERNS THE CONSUMER TO THIRD PARTIES FOR PURPOSES OF TARGETED ADVERTISING, THE CONTROLLER MAY NOT PROCESS THE PERSONAL DATA SUBJECT TO THE OBJECTION FOR SUCH PURPOSE AND SHALL TAKE REASONABLE STEPS TO COMMUNICATE THE CONSUMER'S OBJECTION, UNLESS IT PROVES IMPOSSIBLE OR INVOLVES DISPROPORTIONATE EFFORT, REGARDING ANY FURTHER PROCESSING OF THE CONSUMER'S PERSONAL DATA FOR THE PURPOSES TO ANY THIRD PARTIES TO WHOM THE CONTROLLER SOLD THE CONSUMER'S PERSONAL

DATA FOR THAT PURPOSE. THIRD PARTIES SHALL HONOR OBJECTION REQUESTS PURSUANT TO THIS SECTION RECEIVED FROM THIRD-PARTY CONTROLLERS.

C. IF A CONSUMER OBJECTS TO PROCESSING FOR ANY PURPOSE OTHER THAN TARGETED ADVERTISING, THE CONTROLLER MAY CONTINUE PROCESSING THE PERSONAL DATA SUBJECT TO THE OBJECTION IF THE CONTROLLER CAN DEMONSTRATE A LEGITIMATE GROUND TO PROCESS THAT PERSONAL DATA THAT OVERRIDES THE POTENTIAL RISKS TO THE RIGHTS OF THE CONSUMER ASSOCIATED WITH THE PROCESSING OR IF ANOTHER EXEMPTION IN THIS ARTICLE APPLIES.

18-577. Controller's responsibilities; exceptions

A. A CONTROLLER SHALL COMMUNICATE ANY CORRECTION, DELETION OR RESTRICTION OF PROCESSING CARRIED OUT IN ACCORDANCE WITH THIS ARTICLE TO EACH THIRD-PARTY RECIPIENT TO WHOM THE CONTROLLER KNOWS THE PERSONAL DATA HAS BEEN DISCLOSED, INCLUDING THIRD PARTIES THAT RECEIVED THE DATA THROUGH A SALE, WITHIN ONE YEAR PRECEDING THE VERIFIED REQUEST UNLESS THIS PROVES FUNCTIONALLY IMPRACTICAL OR TECHNICALLY INFEASIBLE OR INVOLVES DISPROPORTIONATE EFFORT OR THE CONTROLLER KNOWS OR IS INFORMED BY THE THIRD PARTY THAT THE THIRD PARTY IS NOT CONTINUING TO USE THE PERSONAL DATA.

B. A CONTROLLER SHALL PROVIDE INFORMATION ON ACTION TAKEN ON A VERIFIED REQUEST UNDER THIS SECTION WITHOUT UNDUE DELAY AND WITHIN THIRTY DAYS AFTER RECEIPT OF THE REQUEST. THE TIME PERIOD MAY BE EXTENDED BY SIXTY ADDITIONAL DAYS IF REASONABLY NECESSARY, TAKING INTO ACCOUNT THE COMPLEXITY AND NUMBER OF THE REQUESTS. THE CONTROLLER SHALL INFORM THE CONSUMER OF ANY SUCH EXTENSION WITHIN THIRTY CALENDAR DAYS AFTER RECEIPT OF THE VERIFIED OR VALIDATED REQUEST, TOGETHER WITH THE REASONS FOR THE DELAY. IF THE CONSUMER MAKES THE VERIFIED OR VALIDATED REQUEST BY ELECTRONIC MEANS, THE INFORMATION MUST BE PROVIDED BY ELECTRONIC MEANS IF POSSIBLE, UNLESS OTHERWISE REQUESTED BY THE CONSUMER.

C. 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 THIRTY DAYS AFTER RECEIPT OF THE REQUEST OF THE REASONS FOR NOT TAKING ACTION AND ANY POSSIBILITY FOR INTERNAL REVIEW OF THE DECISION BY THE CONTROLLER.

D. THE CONTROLLER SHALL PROVIDE INFORMATION UNDER THIS SECTION FREE OF CHARGE TO THE CONSUMER. IF REQUESTS FROM A CONSUMER ARE MANIFESTLY UNFOUNDED OR EXCESSIVE, IN PARTICULAR BECAUSE OF THEIR REPETITIVE CHARACTER, THE CONTROLLER MAY EITHER:

1. CHARGE A REASONABLE FEE TAKING INTO ACCOUNT THE ADMINISTRATIVE COSTS OF PROVIDING THE INFORMATION OR COMMUNICATION OR TAKING THE ACTION REQUESTED.

2. REFUSE TO ACT ON THE REQUEST. THE CONTROLLER BEARS THE BURDEN OF DEMONSTRATING THE MANIFESTLY UNFOUNDED OR EXCESSIVE CHARACTER OF THE REQUEST AND MUST DETAIL THE CATEGORIES OR TYPES OF PERSONAL INFORMATION AND THE EXCESSIVE CHARACTER OR NATURE OF THE REQUEST.

E. IF THE CONTROLLER HAS REASONABLE DOUBTS CONCERNING THE IDENTITY OF THE CONSUMER MAKING A REQUEST UNDER THIS SECTION, THE CONTROLLER MAY REQUEST ADDITIONAL INFORMATION NECESSARY TO CONFIRM THE IDENTITY OF THE CONSUMER.

F. A CONSUMER IS NOT SUBJECT TO A DECISION BASED SOLELY ON PROFILING THAT PRODUCES LEGAL EFFECTS CONCERNING THE CONSUMER OR THAT SIMILARLY SIGNIFICANTLY AFFECTS THE CONSUMER. LEGAL OR SIMILARLY SIGNIFICANT EFFECTS INCLUDE DENIAL OF CONSEQUENTIAL SERVICES OR SUPPORT, SUCH AS FINANCIAL AND LENDING SERVICES, HOUSING, INSURANCE, EDUCATION

ENROLLMENT, CRIMINAL JUSTICE, EMPLOYMENT OPPORTUNITIES AND HEALTH CARE SERVICES.

G. THIS SECTION DOES NOT APPLY IF THE DECISION IS:

- 1. NECESSARY FOR ENTERING INTO OR PERFORMING A CONTRACT BETWEEN THE CONSUMER AND A CONTROLLER.**
- 2. AUTHORIZED BY A FEDERAL, STATE OR LOCAL LAW OR REGULATION TO WHICH THE CONTROLLER IS SUBJECT AND THAT INCORPORATES SUITABLE MEASURES TO SAFEGUARD THE CONSUMER'S RIGHTS AND LEGITIMATE INTERESTS, AS INDICATED BY THE RISK ASSESSMENTS REQUIRED BY THIS ARTICLE.**
- 3. BASED ON THE CONSUMER'S INFORMED CONSENT.**

H. NOTWITHSTANDING SUBSECTION G OF THIS SECTION, THE CONTROLLER SHALL IMPLEMENT SUITABLE MEASURES TO SAFEGUARD CONSUMER RIGHTS AND LEGITIMATE INTERESTS WITH RESPECT TO DECISIONS BASED SOLELY ON PROFILING, INCLUDING PROVIDING HUMAN REVIEW OF THE DECISION, TO EXPRESS THE CONSUMER'S POINT OF VIEW WITH RESPECT TO THE DECISION AND TO CONTEST THE DECISION.

18-578. Enforcement; violation; civil penalty; consumer privacy fund

A. THE ATTORNEY GENERAL MAY BRING AN ACTION IN THE NAME OF THIS STATE, OR AS PARENS PATRIAE, ON BEHALF OF PERSONS RESIDING IN THIS STATE, TO ENFORCE THIS ARTICLE.

B. A CONTROLLER OR PROCESSOR VIOLATES THIS ARTICLE IF THE CONTROLLER OR PROCESSOR FAILS TO CURE ANY ALLEGED BREACH OF THIS ARTICLE WITHIN THIRTY DAYS AFTER RECEIVING NOTICE OF ALLEGED NONCOMPLIANCE. ANY CONTROLLER OR PROCESSOR THAT VIOLATES THIS ARTICLE IS SUBJECT TO AN INJUNCTION AND IS LIABLE FOR A CIVIL PENALTY OF NOT MORE THAN \$2,500 FOR EACH VIOLATION OR \$7,500 FOR EACH INTENTIONAL VIOLATION.

C. THE CONSUMER PRIVACY FUND IS ESTABLISHED CONSISTING OF CIVIL PENALTIES IMPOSED UNDER THIS ARTICLE. THE ATTORNEY GENERAL SHALL ADMINISTER THE FUND. THE MONIES IN THE FUND ARE SUBJECT TO LEGISLATIVE APPROPRIATION.

18-579. State preemption

THE REGULATION OF DATA SECURITY IS OF STATEWIDE CONCERN. THE REGULATION OF DATA SECURITY PURSUANT TO THIS ARTICLE SUPERSEDES ANY LOCAL LAW OR REGULATION AND IS NOT SUBJECT TO FURTHER REGULATION BY A COUNTY, CITY, TOWN OR OTHER POLITICAL SUBDIVISION OF THIS STATE.

18-580. Exceptions

A. THE OBLIGATIONS IMPOSED ON CONTROLLERS OR PROCESSORS UNDER THIS ARTICLE DO NOT RESTRICT A CONTROLLER'S OR PROCESSOR'S ABILITY TO DO ANY OF THE FOLLOWING:

- 1. COMPLY WITH FEDERAL, STATE OR LOCAL LAWS AND REGULATIONS.**
- 2. COMPLY WITH A CIVIL, CRIMINAL OR REGULATORY INQUIRY, INVESTIGATION, SUBPOENA OR SUMMONS BY A FEDERAL, STATE, LOCAL OR OTHER GOVERNMENTAL AUTHORITY.**
- 3. COOPERATE WITH LAW ENFORCEMENT AGENCIES CONCERNING CONDUCT OR ACTIVITY THAT THE CONTROLLER OR PROCESSOR REASONABLY AND IN GOOD FAITH BELIEVES MAY VIOLATE A FEDERAL, STATE OR LOCAL LAW OR REGULATION.**
- 4. INVESTIGATE, EXERCISE OR DEFEND LEGAL CLAIMS.**
- 5. PREVENT OR DETECT IDENTITY THEFT, FRAUD OR OTHER CRIMINAL ACTIVITY OR VERIFY IDENTITIES.**

B. THE OBLIGATIONS IMPOSED ON CONTROLLERS AND PROCESSORS UNDER THIS ARTICLE DO NOT APPLY IF COMPLIANCE BY THE CONTROLLER OR PROCESSOR WITH THIS ARTICLE WOULD VIOLATE AN EVIDENTIARY PRIVILEGE UNDER THE LAWS OF THIS STATE AND DO NOT PREVENT THE CONTROLLER OR PROCESSOR FROM PROVIDING PERSONAL DATA CONCERNING A CONSUMER TO A PERSON COVERED BY

AN EVIDENTIARY PRIVILEGE UNDER THE LAWS OF THIS STATE AS PART OF A PRIVILEGED COMMUNICATION.

C. A CONTROLLER OR PROCESSOR THAT DISCLOSES PERSONAL DATA TO A THIRD-PARTY CONTROLLER OR PROCESSOR IN COMPLIANCE WITH THE REQUIREMENTS OF THIS ARTICLE IS NOT IN VIOLATION OF THIS ARTICLE IF THE THIRD-PARTY RECIPIENT PROCESSES THE PERSONAL DATA IN VIOLATION OF THIS ARTICLE, IF AT THE TIME OF DISCLOSING THE PERSONAL DATA THE DISCLOSING CONTROLLER OR PROCESSOR DID NOT HAVE ACTUAL KNOWLEDGE THAT THE THIRD-PARTY RECIPIENT INTENDED TO COMMIT A VIOLATION. A THIRD-PARTY RECIPIENT THAT RECEIVES PERSONAL DATA FROM A CONTROLLER OR PROCESSOR IS LIKEWISE NOT LIABLE UNDER THIS ARTICLE FOR THE OBLIGATIONS OF A CONTROLLER OR PROCESSOR TO WHICH IT PROVIDES SERVICES.

D. THIS ARTICLE DOES NOT REQUIRE A CONTROLLER OR PROCESSOR TO DO ANY OF THE FOLLOWING:

1. REIDENTIFY DEIDENTIFIED DATA.

2. RETAIN PERSONAL DATA CONCERNING A CONSUMER THAT THE CONTROLLER OR PROCESSOR WOULD NOT OTHERWISE RETAIN IN THE ORDINARY COURSE OF BUSINESS.

3. COMPLY WITH A REQUEST TO EXERCISE ANY OF THE RIGHTS OF THIS ARTICLE IF THE CONTROLLER OR PROCESSOR IS UNABLE TO VERIFY, USING COMMERCIALY REASONABLE EFFORTS, THE IDENTITY OF THE CONSUMER MAKING THE REQUEST.

4. RETAIN PERSONAL DATA BEYOND EXISTING LEGAL OBLIGATIONS, RULES OR LAWS.

E. OBLIGATIONS IMPOSED ON CONTROLLERS AND PROCESSORS UNDER THIS ARTICLE DO NOT:

1. ADVERSELY AFFECT THE RIGHTS OF ANY PERSONS.

2. APPLY TO PROCESSING PERSONAL DATA BY A NATURAL PERSON IN THE COURSE OF A PURELY PERSONAL OR HOUSEHOLD ACTIVITY.

18-581. Liability

A. THIS ARTICLE DOES NOT SERVE AS THE BASIS FOR A PRIVATE RIGHT OF ACTION UNDER THIS ARTICLE OR ANY OTHER LAW.

B. IF MORE THAN ONE CONTROLLER OR PROCESSOR, OR BOTH A CONTROLLER AND A PROCESSOR, INVOLVED IN THE SAME PROCESSING ARE IN VIOLATION OF THIS ARTICLE, THE LIABILITY SHALL BE ALLOCATED AMONG THE PARTIES ACCORDING TO PRINCIPLES OF COMPARATIVE FAULT, UNLESS SUCH LIABILITY IS OTHERWISE ALLOCATED BY CONTRACT AMONG THE PARTIES.

18-582. Applicability

A. THIS ARTICLE APPLIES TO A LEGAL ENTITY WITH AN ANNUAL GROSS REVENUE OF AT LEAST \$25,000,000 THAT CONDUCTS BUSINESS IN THIS STATE OR PRODUCES PRODUCTS OR SERVICES THAT ARE INTENTIONALLY TARGETED TO RESIDENTS OF THIS STATE AND THAT SATISFIES EITHER OF THE FOLLOWING THRESHOLDS:

1. CONTROLS OR PROCESSES DATA OF AT LEAST ONE HUNDRED THOUSAND CONSUMERS.

2. DERIVES OVER THIRTY-FIVE PERCENT OF GROSS REVENUE FROM THE SALE OF PERSONAL INFORMATION AND PROCESSES OR CONTROLS PERSONAL INFORMATION OF AT LEAST TWENTY-FIVE THOUSAND CONSUMERS.

B. THIS ARTICLE DOES NOT APPLY TO:

1. STATE AND LOCAL GOVERNMENTS.

2. PERSONAL DATA SETS TO THE EXTENT THAT THE DATA SETS ARE REGULATED BY THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (P.L. 104-191), THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (P.L. 111-5) OR THE GRAMM-LEACH-BLILEY ACT OF 1999 (P.L. 106-102).

- 3. DATA SETS THAT ARE MAINTAINED FOR EMPLOYMENT RECORDS PURPOSES.**
- 4. BUSINESSES AND ACTIVITIES THAT ARE COVERED BY THE FAIR CREDIT REPORTING ACT (P.L. 90-321).**