

---

---

# A BILL FOR AN ACT

RELATING TO PERSONAL INFORMATION.

**BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:**

1           SECTION 1. The legislature finds that personally  
2           identifiable information maintained by government entities is  
3           increasingly targeted for exfiltration and misuse for financial  
4           fraud, identity theft, and other cybersecurity harms. The  
5           legislature further finds that definitions of personally  
6           identifiable information in State law are fragmented across  
7           chapters and, for certain government entities, do not reflect  
8           current technological realities, including the publication and  
9           indexing of government records through websites, searchable  
10          databases, bulk-download repositories, and application  
11          programming interfaces.

12          The legislature also finds that modern artificial  
13          intelligence systems may treat government records and databases  
14          as trusted sources and may be trained on, summarize, or generate  
15          content derived from those records. When personal information  
16          is publicly accessible through government systems, artificial



1 intelligence tools may inadvertently reproduce that information,  
2 compounding privacy, safety, and cybersecurity risks.

3 Accordingly, the purpose of this Act is to modernize and  
4 standardize protections for personal information maintained by  
5 government entities by:

- 6 (1) Prohibiting government entities from making personal  
7 information publicly accessible through a publicly  
8 accessible information system or publicly accessible  
9 source of information, except under certain  
10 conditions;
- 11 (2) Allowing individuals who reasonably believe their  
12 personal information is publicly accessible through a  
13 government entity's publicly accessible information  
14 system or publicly accessible source of information to  
15 submit a written notice to the entity to require  
16 corrective action;
- 17 (3) Establishing a cause of action to compel compliance;
- 18 (4) Establishing statutory penalties for intentional  
19 noncompliance;



- 1 (5) Requiring government entities to adopt and implement
- 2 policies and procedures to prevent personal
- 3 information from being publicly accessible;
- 4 (6) Requiring government entities that own, license,
- 5 maintain, use, collect, or possess personal
- 6 information to implement and maintain certain
- 7 reasonable security procedures and practices to
- 8 protect the personal information;
- 9 (7) Requiring government entities to provide notice to
- 10 individuals in the case of a breach of a security
- 11 system protecting personal information; and
- 12 (8) Requiring government entities to submit annual reports
- 13 to the legislature.

14 SECTION 2. Chapter 84, Hawaii Revised Statutes, is amended  
 15 by adding a new part to be appropriately designated and to read  
 16 as follows:

17 **"PART . PERSONAL INFORMATION; GOVERNMENT INFORMATION**  
 18 **SECURITY**

19 **§84-A Definitions.** As used in this part:

20 "Government entity" means any department, agency, board,  
 21 commission, authority, or instrumentality of the State or a



1 county, including the legislature and its agencies, the  
2 judiciary and its administrative agencies, the office of  
3 Hawaiian affairs, and any public corporation or other  
4 establishment owned, operated, or managed by or on behalf of the  
5 State or any county.

6 "Genetic data" means any data, regardless of its format,  
7 that results from the analysis of a biological sample of an  
8 individual, or from another source enabling equivalent  
9 information to be obtained, and concerns genetic material.

10 "Health insurance information" means an individual's  
11 insurance policy number or subscriber identification number, any  
12 unique identifier used by a health insurer to identify the  
13 individual, or any information in an individual's application  
14 and claims history, including any appeals records.

15 "Medical information" means any individually identifiable  
16 information, in electronic or physical form, regarding an  
17 individual's medical history or medical treatment or diagnosis  
18 by a health care professional.

19 "Personal information" means an individual's first name or  
20 first initial and last name in combination with any one or more



1 of the following data elements, where either the name or the  
2 data elements are not encrypted or redacted:

- 3 (1) Social security number;
- 4 (2) Driver's license number, state identification card  
5 number, tax identification number, passport number,  
6 military identification number, or other unique  
7 identification number issued on a government document  
8 commonly used to verify the identity of a specific  
9 individual;
- 10 (3) Account number, credit card number, or debit card  
11 number;
- 12 (4) Medical information;
- 13 (5) Health insurance information;
- 14 (6) Unique biometric data generated from measurements or  
15 technical analysis of human body characteristics, such  
16 as a fingerprint, retina, or iris image, used to  
17 authenticate a specific individual; provided that  
18 unique biometric data does not include a physical or  
19 digital photograph, unless used or stored for facial  
20 recognition purposes;
- 21 (7) Genetic data; and



1 (8) A username or electronic mail address in combination  
2 with a password or security question and answer that  
3 would permit access to an online account.

4 "Publicly accessible information system" means any website,  
5 portal, online searchable database, bulk-download repository,  
6 application programming interface, or substantially similar  
7 system that is made available to the public by a government  
8 entity without individualized authorization.

9 "Publicly accessible source of information" includes any  
10 document, record, image, dataset, or other information that is  
11 posted, published, indexed, or otherwise made available to the  
12 public through a publicly accessible information system.

13 "Redact" means to remove or obscure personal information so  
14 that it is not readable, not retrievable, and not usable by the  
15 public.

16 "Reasonable security procedures and practices" means  
17 security procedures and practices appropriate to the nature of  
18 the personal information, consistent with section 84-I.

19 **§84-B Public posting of personal information; prohibition;**  
20 **publicly accessible information systems.** (a) A government  
21 entity shall not make personal information publicly accessible



1 through a publicly accessible information system or publicly  
2 accessible source of information unless a federal or state  
3 statute, a rule adopted pursuant to statute, or a court order  
4 explicitly requires that the specific item of personal  
5 information be made publicly accessible.

6 (b) The obligation to disclose a government record under  
7 chapter 92F or any other law shall not, by itself, be construed  
8 to require a government entity to make personal information  
9 publicly accessible through a publicly accessible information  
10 system.

11 (c) Nothing in this part shall be construed to limit  
12 disclosure of government records as required by law; provided  
13 that a government entity shall employ redaction or sanitization  
14 to prevent public accessibility of personal information through  
15 publicly accessible information systems unless explicitly  
16 required under subsection (a).

17 (d) With respect to account numbers, credit card numbers,  
18 and debit card numbers, a government entity shall not make  
19 publicly accessible any portion of the number, whether in full  
20 or in part, unless explicitly required under subsection (a);  
21 provided that a government entity may make publicly accessible a



1 truncated number consisting only of the last four digits when  
2 the truncated number is reasonably necessary to identify a  
3 transaction or account reflected in a government record and no  
4 other personal information is made publicly accessible in  
5 connection with the truncated number.

6 (e) Each government entity shall implement and maintain  
7 processes designed to reduce the inadvertent public  
8 accessibility of personal information, including controls over  
9 posting, indexing, bulk downloads, and application programming  
10 interfaces, and reasonable measures to detect and remediate  
11 inadvertent public accessibility in publicly accessible  
12 information systems.

13 (f) For the purposes of this section, "make publicly  
14 accessible" includes publishing, posting, displaying, indexing,  
15 enabling search, enabling bulk download, or otherwise providing  
16 public access through any publicly accessible information system  
17 or publicly accessible source of information, including in text,  
18 image, scanned document, portable document format file, or other  
19 file format.

20 **§84-C Notice of publicly accessible personal information;**  
21 **acknowledgement; corrective action.** (a) Any individual who



1 reasonably believes that the individual's personal information  
2 is publicly accessible through a publicly accessible information  
3 system or publicly accessible source of information controlled  
4 by a government entity may submit a written notice to the  
5 government entity identifying, to the extent reasonably  
6 practicable, the location of the publicly accessible personal  
7 information.

8 (b) Within three business days after receipt of a written  
9 notice under subsection (a), the government entity shall provide  
10 a written acknowledgement to the individual and shall commence  
11 corrective action.

12 (c) A government entity shall complete corrective action  
13 within thirty days after receipt of a written notice under  
14 subsection (a) by removing, redacting, or otherwise sanitizing  
15 the personal information so that it is not publicly accessible;  
16 provided that this section shall not require removal or  
17 redaction of information that is explicitly required to be  
18 publicly accessible under section 84-B(a).

19 (d) Corrective action under this section shall be limited  
20 to the minimum necessary to remove public accessibility of the



1 personal information and shall not require deletion of non-  
2 personal information.

3       **§84-D Extension of time to complete corrective action.** A  
4 government entity that receives a valid written notice pursuant  
5 to section 84-C and requires additional time to complete  
6 corrective action may extend the time to complete corrective  
7 action by providing written notice to the individual within  
8 three business days after receipt of the written notice. An  
9 extension under this section may be for up to an additional ten  
10 business days; provided that the extension shall not extend the  
11 thirty-day period under section 84-C.

12       **§84-E Civil remedies.** (a) After providing written notice  
13 under section 84-C and allowing the government entity thirty  
14 days to complete corrective action, an individual whose personal  
15 information remains publicly accessible in violation of this  
16 part may bring an action for injunctive relief in the circuit  
17 court of competent jurisdiction to compel compliance.

18       (b) If the court finds that the government entity  
19 intentionally refused to take corrective action after receipt of  
20 a valid written notice, the court may, in addition to injunctive  
21 relief, award:



1 (1) Statutory damages of not less than \$1,000 and not more  
2 than \$5,000 per instance of intentional refusal; and

3 (2) Reasonable attorneys' fees and costs.

4 (c) This section shall not be construed to create a cause  
5 of action for monetary damages for negligent failure to complete  
6 corrective action, except as provided in subsection (b).

7 **§84-F Exceptions; construction.** (a) This part shall not  
8 apply to personal information that an individual voluntarily  
9 publishes on the Internet after the effective date of this Act.

10 (b) This part shall not be construed to require removal or  
11 redaction of information that is explicitly required to be  
12 publicly accessible under section 84-B(a).

13 (c) This part shall be construed to reduce public exposure  
14 of personal information through publicly accessible information  
15 systems while preserving access to government records as  
16 provided by law.

17 **§84-G Policies; internal controls.** Each government entity  
18 shall adopt and implement policies and procedures necessary to  
19 comply with this part, including policies governing public  
20 posting, redaction, sanitization, access controls for publicly  
21 accessible information systems, and incident response.



1           **§84-H Government records.** (a) Nothing in this part shall  
2 be construed to alter rights to access government records under  
3 chapter 92F or any other law.

4           (b) When a government entity discloses government records  
5 through a publicly accessible information system, the government  
6 entity shall not make personal information publicly accessible  
7 unless explicitly required under section 84-B(a).

8           **§84-I Reasonable security procedures and practices;  
9 contractors; incident reporting.** (a) A government entity that  
10 owns, licenses, maintains, uses, collects, or possesses personal  
11 information about an individual shall implement and maintain  
12 reasonable security procedures and practices appropriate to the  
13 nature of the personal information, to protect the personal  
14 information from unauthorized access, destruction, use,  
15 modification, or disclosure.

16           (b) A government entity that discloses personal  
17 information to a contractor or other third party for the purpose  
18 of performing services on behalf of the government entity shall  
19 require, by contract, that the contractor or third party:



- 1 (1) Implement and maintain reasonable security procedures  
2 and practices appropriate to the nature of the  
3 personal information;
- 4 (2) Report any breach of the security of the system, or  
5 suspected breach involving personal information, to  
6 the government entity as soon as practicable, but in  
7 no event later than seventy-two hours after discovery;
- 8 (3) Cooperate with investigation, containment, and  
9 notification obligations;
- 10 (4) Require the same or substantially similar obligations  
11 to be imposed on subcontractors or subservice  
12 providers;
- 13 (5) Provide, upon request, reasonable assurances of  
14 compliance, including audit rights or independent  
15 attestations aligned with commonly accepted security  
16 frameworks, including Systems and Organizations  
17 Controls 2 (SOC 2) or National Institute of Standards  
18 and Technology (NIST)-based controls; and
- 19 (6) Minimize the personal information processed for the  
20 contract and, upon completion or termination of the  
21 contract, return or securely destroy personal



1 information, subject to any legal retention  
2 requirements.

3 **§84-J Breach of security of system; notice.** (a) In the  
4 case of a breach of the security of the system involving  
5 personal information, a government entity that owns or licenses  
6 computerized data that includes personal information shall  
7 disclose the breach following discovery or notification of the  
8 breach to any resident of the State whose unencrypted personal  
9 information was, or is reasonably believed to have been,  
10 acquired by an unauthorized person, in the most expedient time  
11 possible and without unreasonable delay, consistent with the  
12 legitimate needs of law enforcement or any measures necessary to  
13 determine the scope of the breach and restore the reasonable  
14 integrity of the system.

15 (b) Notification may be delayed if a law enforcement  
16 agency determines that notification will impede a criminal  
17 investigation. Notification shall be made promptly after the  
18 law enforcement agency determines that notification will not  
19 compromise the investigation.



1 (c) The notification required by this section shall be  
2 written in plain language, titled "Notice of Data Breach", and  
3 present the information under the following headings:

- 4 (1) "What Happened?";
- 5 (2) "What Information Was Involved?";
- 6 (3) "What We Are Doing.";
- 7 (4) "What You Can Do."; and
- 8 (5) "For More Information.".

9 (d) The notification required by this section shall  
10 include, at a minimum:

- 11 (1) The name and contact information of the reporting  
12 government entity;
- 13 (2) A list of the types of personal information that were,  
14 or are reasonably believed to have been, the subject  
15 of a breach;
- 16 (3) If available at the time of notice, the date of the  
17 breach, the estimated date of the breach, or the date  
18 range within which the breach occurred;
- 19 (4) Whether notification was delayed as a result of a law  
20 enforcement investigation;



- 1 (5) A general description of the breach incident,  
2 described in a manner that does not compromise  
3 security controls;
- 4 (6) The toll-free telephone numbers and addresses of the  
5 major credit reporting agencies, if the breach exposed  
6 information that could be used for identity theft; and
- 7 (7) If the breach exposed a social security number or a  
8 driver's license or state identification card number,  
9 advice to the affected individual to remain vigilant  
10 by reviewing account statements and monitoring free  
11 credit reports.
- 12 (e) Notice under this section may be provided by written  
13 notice, electronic notice if consistent with applicable law, or  
14 substitute notice if the government entity demonstrates that the  
15 cost of providing notice would exceed an amount specified by  
16 rule or that the affected class of persons to be notified  
17 exceeds a number specified by rule; provided that substitute  
18 notice shall include, at a minimum, email notice when available,  
19 conspicuous posting on the government entity's website, and  
20 notification to major statewide media.



1 (f) A government entity shall maintain records of breaches  
2 and notices provided under this section for five years.

3 (g) For the purposes of this section, "breach of the  
4 security of the system" means unauthorized acquisition of  
5 computerized data that compromises the security,  
6 confidentiality, or integrity of personal information maintained  
7 by the government entity; provided that good faith acquisition  
8 of personal information by an employee or agent of the  
9 government entity for the purposes of the government entity is  
10 not a breach of the security of the system; provided further  
11 that the personal information is not used or subject to further  
12 unauthorized disclosure.

13 **§84-K Compliance with this part; annual reporting**  
14 **requirement.** Each government entity shall submit an annual  
15 report detailing compliance with this part to the legislature no  
16 later than twenty days prior to the convening of each regular  
17 session.

18 **§84-L Office of Hawaiian affairs, public corporations, and**  
19 **other establishments; applicability of part.** For the office of  
20 Hawaiian affairs, public corporations, and other establishments,  
21 the requirements of this part shall apply only to publicly



1 accessible information systems and publicly accessible sources  
2 of information."

3 SECTION 3. Chapter 92H, Hawaii Revised Statutes, is  
4 amended by adding a new section to be appropriately designated  
5 and to read as follows:

6 "§92H- Relationship to part of chapter 84. Nothing  
7 in this chapter shall be construed to limit or impair the  
8 requirements of part of chapter 84."

9 SECTION 4. Chapter 84, Hawaii Revised Statutes, is amended  
10 by amending its title to read as follows:

11 "CHAPTER 84  
12 STANDARDS OF CONDUCT; GOVERNMENT INFORMATION SECURITY"

13 SECTION 5. In codifying the new sections added by  
14 section 2 of this Act, the revisor of statutes shall substitute  
15 appropriate section numbers for the letters used in designating  
16 the new sections in this Act.

17 SECTION 6. New statutory material is underscored.

18 SECTION 7. This Act shall take effect on January 1, 2525.



**Report Title:**

Personal Information; Government Entities; Publicly Accessible Information Systems; Publication Controls; Data Security; Notification; Cause of Action; Reports

**Description:**

Prohibits government entities from making personal information publicly accessible through a publicly accessible information system or publicly accessible source of information, except under certain conditions. Allows individuals who reasonably believe their personal information is publicly accessible through a government entity's publicly accessible information system or publicly accessible source of information to submit a written notice to the entity to require corrective action. Establishes a cause of action to compel compliance. Establishes statutory penalties for intentional noncompliance. Requires government entities to adopt and implement policies and procedures to prevent personal information from being publicly accessible. Requires government entities that own, license, maintain, use, collect, or possess personal information to implement and maintain certain reasonable security procedures and practices to protect the personal information. Requires government entities to provide notice to individuals in the case of a breach of a security system protecting personal information. Requires government entities to submit an annual report to the Legislature. Effective 1/1/2525. (SD1)

*The summary description of legislation appearing on this page is for informational purposes only and is not legislation or evidence of legislative intent.*

