

---

---

# A BILL FOR AN ACT

RELATING TO SOCIAL MEDIA.

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

1 SECTION 1. This Act shall be known and may be cited as the  
2 Hawaii Social Media Data Deletion Act.

3 SECTION 2. The legislature finds that social media  
4 platforms collect, store, and process large amounts of users'  
5 personal information, including data that can persist  
6 indefinitely even after a user deletes an account. Users should  
7 have meaningful control over their digital identities and  
8 personal information, including clear rights to delete such  
9 information when they choose to discontinue using a platform.  
10 Effective deletion of personal data upon account termination  
11 promotes digital privacy, reduces the risk of unauthorized data  
12 retention and third-party sharing, and aligns with emerging  
13 state privacy standards.

14 The purpose of this Act is to require certain social media  
15 platforms to:

16 (1) Provide an accessible mechanism for users to delete  
17 their accounts;



1 (2) Permanently delete all personal information and  
2 sensitive personal information associated with deleted  
3 accounts; and

4 (3) Prohibit deceptive practices that obstruct deletion.

5 SECTION 3. The Hawaii Revised Statutes is amended by  
6 adding a new chapter to be appropriately designated and to read  
7 as follows:

8 "CHAPTER

9 SOCIAL MEDIA PROTECTIONS

10 PART I. GENERAL PROVISIONS

11 § -1 **Definitions.** As used in this chapter:

12 "Covered platform" means a social media platform that:

13 (1) Has one million or more monthly active users  
14 nationwide; or

15 (2) Generates \$25,000,000 or more in annual gross  
16 revenues.

17 "Delete" or "deletion" means, to the extent technically  
18 feasible, the removal of personal information and sensitive  
19 personal information from a covered platform's systems and  
20 databases resulting in the covered platform no longer retaining  
21 or using the personal information and sensitive personal



1 information, except as otherwise permitted under applicable  
2 federal or state law.

3 "Education information" means information that is not  
4 publicly available personally identifiable information as  
5 defined in the Family Educational Rights and Privacy Act of 1974  
6 (20 U.S.C. 1232g; 34 C.F.R. part 99).

7 "Neural data" means information that is generated by  
8 measuring the activity of a consumer's central or peripheral  
9 nervous system, and that is not inferred from nonneural  
10 information.

11 "Personal information" means information that identifies,  
12 relates to, describes, is reasonably capable of being associated  
13 with, or could reasonably be linked, directly or indirectly,  
14 with a particular consumer or household. "Personal information"  
15 includes but is not limited to the following if it identifies,  
16 relates to, describes, is reasonably capable of being associated  
17 with, or could be reasonably linked, directly or indirectly,  
18 with a particular consumer or household:

19 (1) Identifiers, such as a real name, alias, postal  
20 address, unique personal identifier, online  
21 identifier, Internet Protocol address, electronic mail



- 1 address, account name, social security number,  
2 driver's license number, passport number, or other  
3 similar identifiers;
- 4 (2) Any personal information described in section 487N-1;
- 5 (3) Characteristics of protected classifications under  
6 federal or state law;
- 7 (4) Commercial information, including records of personal  
8 property, products or services purchased, obtained, or  
9 considered, or other purchasing or consuming histories  
10 or tendencies;
- 11 (5) Biometric information;
- 12 (6) Internet or other electronic network activity  
13 information, including but not limited to browsing  
14 history, search history, and information regarding a  
15 consumer's interaction with an internet website  
16 application, or advertisement;
- 17 (7) Geolocation data;
- 18 (8) Audio, electronic, visual, thermal, olfactory, or  
19 similar information;
- 20 (9) Professional or employment-related information;
- 21 (10) Education information;



1           (11) Inferences drawn from any of the information  
2                    identified in this definition to create a profile  
3                    about a consumer reflecting the consumer's  
4                    preferences, characteristics, psychological trends,  
5                    predispositions, behavior, attitudes, intelligence,  
6                    abilities, and aptitudes; and

7           (12) Sensitive personal information.

8 "Personal information" does not include publicly available  
9 information or lawfully obtained, truthful information that is a  
10 matter of public concern.

11           "Publicly available" means any of the following:

12           (1) Information that is lawfully made available from  
13                    federal, state, or local government records;

14           (2) Information that a business has a reasonable basis to  
15                    believe is lawfully made available to the general  
16                    public by the consumer or from widely distributed  
17                    media; and

18           (3) Information made available by a person to whom the  
19                    consumer has disclosed the information if the consumer  
20                    has not restricted the information to a specific  
21                    audience.



1 "Publicly available" does not include biometric information  
2 collected by a business about a consumer without the consumer's  
3 knowledge.

4 "Sensitive personal information" means:

5 (1) Personal information that reveals:

6 (A) A consumer's social security, driver's license,  
7 state identification card, or passport number;

8 (B) A consumer's account log-in, financial account,  
9 debit card, or credit card number in combination  
10 with any required security or access code,  
11 password, or credentials allowing access to an  
12 account;

13 (C) A consumer's precise geolocation;

14 (D) A consumer's racial or ethnic origin, citizenship  
15 or immigration status, religious or philosophical  
16 beliefs, or union membership;

17 (E) The contents of a consumer's mail, electronic  
18 mail, and text messages, unless the business is  
19 the intended recipient of the communication;

20 (F) A consumer's genetic data; or

21 (G) A consumer's neural data;



- 1 (2) The processing of biometric information for the  
2 purpose of uniquely identifying a consumer;
- 3 (3) Personal information collected and analyzed concerning  
4 a consumer's health; and
- 5 (4) Personal information collected and analyzed concerning  
6 a consumer's sex life or sexual orientation.

7 "Social media platform" means an electronic service or  
8 system that enables users to create profiles and interact with  
9 others, including posting content, messaging, or engaging in  
10 social networking online.

11 "User" means a natural person who is a resident of the  
12 State acting in an individual or household context.

13 **PART II. COVERED PLATFORMS' OBLIGATIONS**

14 **§ -11 Account deletion; user rights.** (a) A covered  
15 platform shall provide every user of the covered platform with a  
16 clear, conspicuous, and easily accessible method to request  
17 deletion of the user's account at any time.

18 (b) Upon confirmation of a user's request for account  
19 deletion, the covered platform shall:

- 20 (1) Archive and delete all personal information and  
21 sensitive personal information associated with the



1 user's account and collected directly through the  
2 user's activity on the covered platform in accordance  
3 with section -12; and

4 (2) Notify the user that deletion of the user's account,  
5 personal information, and sensitive personal  
6 information has been completed.

7 (c) A covered platform shall not design or implement user  
8 interfaces, terms, or processes that:

9 (1) Obscure, delay, or make the request for deletion of a  
10 user's account, personal information, and sensitive  
11 personal information more difficult; or

12 (2) Require disclosure of additional personal information  
13 or sensitive personal information beyond what is  
14 necessary to verify the user's account deletion  
15 request.

16 § -12 Account deletion; verification; timely deletion.

17 (a) Except as provided in subsection (b), a covered platform  
18 shall:

19 (1) Archive and not make publicly accessible the user's  
20 personal information and sensitive personal



1 information for a period of no less than forty-five  
2 days; and

3 (2) Delete the user's personal information and sensitive  
4 personal information no later than ninety days,  
5 after receiving a user's confirmed request to delete the  
6 account, unless otherwise required by federal or state law.

7 (b) A law enforcement agency may direct a covered  
8 platform, pursuant to an approved criminal investigation with an  
9 active case number not to delete a user's personal information  
10 or sensitive personal information and. Upon receiving such  
11 direction, the covered platform shall retain the personal  
12 information or sensitive personal information solely to allow  
13 the law enforcement agency to obtain a court-issued subpoena,  
14 order, or warrant to obtain the user's personal information or  
15 sensitive personal information. A covered platform that has  
16 received direction from a law enforcement agency not to delete  
17 the user's personal information or sensitive personal  
18 information shall not use the user's personal information or  
19 sensitive personal information for any purpose other than  
20 retaining it to produce to the law enforcement agency in  
21 response to a court-issued subpoena, order, or warrant.



1 (c) A covered platform may implement reasonable procedures  
2 to verify that the individual initiating a request for account  
3 deletion is the account holder.

4 § -13 **Recordkeeping.** A covered platform shall maintain  
5 deletion request records and any related compliance  
6 documentation for four years for enforcement and evidentiary  
7 purposes.

8 **PART III. ADMINISTRATION AND ENFORCEMENT**

9 § -21 **Enforcement.** The attorney general may enforce  
10 this chapter through civil actions and seek injunctive relief  
11 and civil penalties for violations of this chapter. Civil  
12 penalties may include fines up to \$ per violation per  
13 day.

14 § -22 **Rules.** The department of the attorney general may  
15 adopt rules pursuant to chapter 91 necessary to implement and  
16 enforce this chapter."

17 SECTION 4. This Act does not affect rights and duties that  
18 matured, penalties that were incurred, and proceedings that were  
19 begun before its effective date.

20 SECTION 5. If any provision of this Act, or the  
21 application thereof to any person or circumstance, is held



1 invalid, the invalidity does not affect other provisions or  
2 applications of the Act that can be given effect without the  
3 invalid provision or application, and to this end the provisions  
4 of this Act are severable.

5 SECTION 6. This Act shall take effect on July 1, 3000.



**Report Title:**

AG; Social Media Platforms; User Accounts; Personal Information;  
Sensitive Personal Information; Deletion; Deceptive Practices

**Description:**

Requires certain social media platforms to provide an accessible mechanism for users to delete their accounts on the platform and permanently erase all personal information and sensitive personal information associated with deleted accounts. Prohibits certain deceptive practices by social media platforms that obstruct the deletion of user accounts. Authorizes the Attorney General to pursue civil actions and seek injunctive relief and penalties for violations. Effective 7/1/3000. (HD2)

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

