
SENATE BILL 6187

State of Washington

66th Legislature

2020 Regular Session

By Senator Zeiger

Prefiled 01/09/20.

1 AN ACT Relating to modifying the definition of personal
2 information for notifying the public about data breaches of a state
3 or local agency system; and amending RCW 42.56.590.

4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

5 **Sec. 1.** RCW 42.56.590 and 2019 c 241 s 5 are each amended to
6 read as follows:

7 (1) Any agency that owns or licenses data that includes personal
8 information shall disclose any breach of the security of the system
9 to any resident of this state whose personal information was, or is
10 reasonably believed to have been, acquired by an unauthorized person
11 and the personal information was not secured. Notice is not required
12 if the breach of the security of the system is not reasonably likely
13 to subject consumers to a risk of harm. The breach of secured
14 personal information must be disclosed if the information acquired
15 and accessed is not secured during a security breach or if the
16 confidential process, encryption key, or other means to decipher the
17 secured information was acquired by an unauthorized person.

18 (2) Any agency that maintains or possesses data that may include
19 personal information that the agency does not own or license shall
20 notify the owner or licensee of the information of any breach of the
21 security of the data immediately following discovery, if the personal

1 information was, or is reasonably believed to have been, acquired by
2 an unauthorized person.

3 (3) The notification required by this section may be delayed if
4 the data owner or licensee contacts a law enforcement agency after
5 discovery of a breach of the security of the system and a law
6 enforcement agency determines that the notification will impede a
7 criminal investigation. The notification required by this section
8 shall be made after the law enforcement agency determines that it
9 will not compromise the investigation.

10 (4) For purposes of this section and except under subsection (5)
11 of this section and RCW 42.56.592, notice may be provided by one of
12 the following methods:

13 (a) Written notice;

14 (b) Electronic notice, if the notice provided is consistent with
15 the provisions regarding electronic records and signatures set forth
16 in 15 U.S.C. Sec. 7001; or

17 (c) Substitute notice, if the agency demonstrates that the cost
18 of providing notice would exceed two hundred fifty thousand dollars,
19 or that the affected class of subject persons to be notified exceeds
20 five hundred thousand, or the agency does not have sufficient contact
21 information. Substitute notice shall consist of all of the following:

22 (i) Email notice when the agency has an email address for the
23 subject persons;

24 (ii) Conspicuous posting of the notice on the agency's web site
25 page, if the agency maintains one; and

26 (iii) Notification to major statewide media.

27 (5) An agency that maintains its own notification procedures as
28 part of an information security policy for the treatment of personal
29 information and is otherwise consistent with the timing requirements
30 of this section is in compliance with the notification requirements
31 of this section if it notifies subject persons in accordance with its
32 policies in the event of a breach of security of the system.

33 (6) Any agency that is required to issue notification pursuant to
34 this section shall meet all of the following requirements:

35 (a) The notification must be written in plain language; and

36 (b) The notification must include, at a minimum, the following
37 information:

38 (i) The name and contact information of the reporting agency
39 subject to this section;

1 (ii) A list of the types of personal information that were or are
2 reasonably believed to have been the subject of a breach;

3 (iii) A time frame of exposure, if known, including the date of
4 the breach and the date of the discovery of the breach; and

5 (iv) The toll-free telephone numbers and addresses of the major
6 credit reporting agencies if the breach exposed personal information.

7 (7) Any agency that is required to issue a notification pursuant
8 to this section to more than five hundred Washington residents as a
9 result of a single breach shall notify the attorney general of the
10 breach no more than thirty days after the breach was discovered.

11 (a) The notice to the attorney general must include the following
12 information:

13 (i) The number of Washington residents affected by the breach, or
14 an estimate if the exact number is not known;

15 (ii) A list of the types of personal information that were or are
16 reasonably believed to have been the subject of a breach;

17 (iii) A time frame of exposure, if known, including the date of
18 the breach and the date of the discovery of the breach;

19 (iv) A summary of steps taken to contain the breach; and

20 (v) A single sample copy of the security breach notification,
21 excluding any personally identifiable information.

22 (b) The notice to the attorney general must be updated if any of
23 the information identified in (a) of this subsection is unknown at
24 the time notice is due.

25 (8) Notification to affected individuals must be made in the most
26 expedient time possible, without unreasonable delay, and no more than
27 thirty calendar days after the breach was discovered, unless the
28 delay is at the request of law enforcement as provided in subsection
29 (3) of this section, or the delay is due to any measures necessary to
30 determine the scope of the breach and restore the reasonable
31 integrity of the data system. An agency may delay notification to the
32 consumer for up to an additional fourteen days to allow for
33 notification to be translated into the primary language of the
34 affected consumers.

35 (9) For purposes of this section, "breach of the security of the
36 system" means unauthorized acquisition of data that compromises the
37 security, confidentiality, or integrity of personal information
38 maintained by the agency. Good faith acquisition of personal
39 information by an employee or agent of the agency for the purposes of
40 the agency is not a breach of the security of the system when the

1 personal information is not used or subject to further unauthorized
2 disclosure.

3 (10)(a) For purposes of this section, "personal information"
4 means:

5 (i) An individual's first name or first initial and last name in
6 combination with any one or more of the following data elements:

7 (A) Social security number or the last four digits of the social
8 security number;

9 (B) Driver's license number or Washington identification card
10 number;

11 (C) Account number, credit or debit card number, or any required
12 security code, access code, or password that would permit access to
13 an individual's financial account, or any other numbers or
14 information that can be used to access a person's financial account;

15 (D) Full date of birth;

16 (E) Private key that is unique to an individual and that is used
17 to authenticate or sign an electronic record;

18 (F) Student, military, or passport identification number;

19 (G) Health insurance policy number or health insurance
20 identification number;

21 (H) Any information about a consumer's medical history or mental
22 or physical condition or about a health care professional's medical
23 diagnosis or treatment of the consumer; or

24 (I) Biometric data generated by automatic measurements of an
25 individual's biological characteristics, such as a fingerprint,
26 voiceprint, eye retinas, irises, or other unique biological patterns
27 or characteristics that is used to identify a specific individual;

28 (ii) User name or email address in combination with a password or
29 security questions and answers that would permit access to an online
30 account; and

31 (iii) Any of the data elements or any combination of the data
32 elements described in (a)(i) of this subsection without the
33 consumer's first name or first initial and last name if:

34 (A) Encryption, redaction, or other methods have not rendered the
35 data element or combination of data elements unusable; and

36 (B) The data element or combination of data elements would enable
37 a person to commit identity theft against a consumer.

38 (b) Personal information does not include publicly available
39 information that is lawfully made available to the general public
40 from federal, state, or local government records.

1 (11) For purposes of this section, "secured" means encrypted in a
2 manner that meets or exceeds the national institute of standards and
3 technology standard or is otherwise modified so that the personal
4 information is rendered unreadable, unusable, or undecipherable by an
5 unauthorized person.

--- **END** ---