Wisconsin Legislative Council
AMENDMENT MEMO

Memo published: November 15, 2023

Contact: Abby Gorzlancyk, Staff Attorney

2023 Assembly Bill 466

Assembly Amendment 1, Assembly Amendment 1 to Assembly Amendment 1, and Assembly Amendment 2 to Assembly Amendment 1

2023 ASSEMBLY BILL 466

2023 Assembly Bill 466 gives a consumer certain rights over their personal data and imposes certain obligations on any controller and processor of personal data. The bill applies to a person that conducts business in Wisconsin or produces products or services that are targeted to residents of this state that meet either of the following: (1) during a calendar year, controls or processes the personal data of at least 100,000 consumers; or (2) controls or processes personal data of at least 25,000 consumers and derives over 50 percent of its gross revenue from the sale of personal data. The provisions of the bill specifically do not apply to listed organizations,[1] listed data including certain data governed by federal law,[2] and de-identified data.[3]

Consumers

The bill defines a consumer as "an individual who is a resident of this state, acting only in an individual or household context" and specifically does not include "an individual acting in a commercial or employment context." Under the bill, a consumer has the following rights to:

- Confirm whether or not a controller is processing their personal data and to access such data;
- Correct inaccuracies in their own collected personal data;
- Delete personal data provided by or obtained about the consumer;
- Obtain a copy of their personal data that is portable; and

[1] The listed entities exempt from the bill are government entities, financial institutions or its affiliates subject to Title V of the federal Gram-Leach-Bliley Act, a covered entity or business associate governed by the Health Insurance Portability and Accountability Act (HIPAA) or Health Information Technology for Economic and Clinical Health (HITECH), a nonprofit organization, an institution of higher education, an entity under contract under s. 153.05 (2r), Stats., and its contractors, and the data organized under contract under s. 135.05 (2r), Stats., and its contractors.

[2] Some of the data exempted from the bill's requirements include health care information or records governed by HIPAA, HITECH, Cures Act, or other similar laws, health care information protected by state statute, information created for purposes of the Health Care Quality Improvement Act, patient safety work product for the purposes of the Patient Safety and Quality Improvement Act, personal information on credit worthiness protected by the Fair Credit Reporting Act, personal data regulated by the Family Educational Rights and Privacy Act, and personal data regulated by the Farm Credit Act.

[3] The bill defines de-identified data as "data that cannot be reasonably linked to an identified or identifiable individual, or device linked to such a person."

- Opt out of the processing of personal data for targeted advertising, sale, or profiling.

A consumer can enforce these rights by making a request to a data controller who must respond within 45 days and have a mechanism for a consumer to appeal their responses.

Controllers

The bill defines a controller as "a person that, alone or jointly with others, determines the purpose and means of processing personal data." Under the bill, a controller must abide by the following responsibilities:

- Limit the collection of personal data to what is adequate, relevant, and reasonably necessary;
- Cannot process data for purposes that are not reasonably necessary and not compatible with the disclosed purposes for processing data;
- Maintain reasonable data security practices;
- Cannot discriminate against a consumer who is exercising their rights under the bill, except the controller can offer different prices, quality, or selection based on the consumer opting out of data collection or participating in a rewards program;
- Cannot process sensitive data without a consumer's consent;
- Must provide the consumer with a reasonably accessible, clear, and meaningful privacy notice; and
- Must conspicuously disclose if they sell personal data to third parties for targeted advertising.

Controllers must also conduct data protection assessments.

Processors

The bill defines a processor as "an individual or person that processes personal data on behalf of a controller." Under the bill, a processor must adhere to the directions of the controller and assist the controller in meeting the requirements of the bill, respond to consumer rights requests, maintain security of personal data, and conduct data protection assessments. The bill requires the contractual agreement between the controller and processor to address the following:

- Ensure each person processing personal data is subject to a duty of confidentiality;
- The processor must delete or return all personal data to the controller as requested;
- The processor must make the controller aware of its compliance with the bill's requirements; and
- The processor must either allow reasonable assessments by the controller or arrange for a qualified and independent assessor to conduct assessments of its compliance with the bill.

Enforcement

The bill provides that its provisions are exclusively enforced through the Attorney General who must give entities 30 days written notice of potential violations. If within 30 days the controller or processor cures the noticed violation and provides the Attorney General an express written statement that the alleged violations have been cured and no further violations will occur, no action for statutory damages can be initiated. However, if the controller or processor continues the violation, the Attorney General can initiate an action and seek an injunction and damages for up to $7,500 for each violation along with reasonable expenses incurred.

ASSEMBLY AMENDMENT 1

Assembly Amendment 1 places the bill's provisions within ch. 100, Stats., which is administered by the Department of Agriculture, Trade, and Consumer Protection (DATCP) and permits DATCP to promulgate rules necessary to effect the purposes of the bill. Relatedly, the amendment empowers both DATCP and the Department of Justice (DOJ) with authority to enforce violations of the bill and authority to serve subpoenas, complaints, orders, and other demands. The amendment gives DOJ sole authority to use civil investigative demands and changes the civil forfeitures to a range of $100 to $10,000 per violation. The amendment sunsets the provision allowing a controller or processor who has been notified of an alleged violation the right to cure the violation within 30 days on June 30, 2031.

Assembly Amendment 1 also modifies two definitions in the bill. First, the amendment changes the definition of consent to specifically not include general terms-of-use agreements, hovering over, muting, pausing, or closing a piece of content, or agreement by use of a dark pattern[4] or other form of screen manipulation. Second, the amendment changes the definition of sale of personal data to include sale for monetary or other value.

Lastly, the amendment allows "a controller that recognizes signals approved by other states" to be in compliance with the privacy notice requirement of a controller as long as certain criteria are met. First, there must be a clear and conspicuous link on the controller's website that enables a consumer to opt out of targeted advertising or sale of their personal data. Second, an opt-out preference signal is sent with the consumer's consent by a technology or other mechanism to the controller to indicate the consumer's intent to opt out of processing their personal data for the purpose of targeted advertising or sale. The technology utilized must do all of the following: (1) not unfairly advantage one controller over another; (2) require the consumer to make an affirmative and unambiguous choice to opt out of any processing of the consumer's personal data; (3) be easy to use by the average consumer; and (4) enable the controller to accurately determine whether the consumer is a resident of Wisconsin and has made a legitimate request to opt out of targeted advertising or sale of their personal data.

ASSEMBLY AMENDMENT 1 TO ASSEMBLY AMENDMENT 1

Assembly Amendment 1 to Assembly Amendment 1 generally reorganizes portions of the enforcement section of the bill without altering DATCP or DOJ's authorities to enforce and serve complaints, notices, orders, demands, or subpoenas. The amendment adds injunction as a possible penalty for violations of the bill, in addition to the civil forfeitures. Additionally, the amendment changes the written notice and 30 days to cure sunset date from July 1, 2031, to July 1, 2029.

ASSEMBLY AMENDMENT 2 TO ASSEMBLY AMENDMENT 1

Assembly Amendment 2 to Assembly Amendment 1 removes the explicit rulemaking authority granted to DATCP under Assembly Amendment 1.

BILL HISTORY

Representative Zimmerman offered Assembly Amendment 1 on October 10, 2023, Assembly Amendment 1 to Assembly Amendment 1 on October 31, 2023, and Assembly Amendment 2 to Assembly Amendment 1 on November 13, 2023. On November 14, 2023, the Assembly voted to adopt

[4] The amendment defines dark patterns to mean "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice."

Assembly Amendment 1 to Assembly Amendment 1, Assembly Amendment 2 to Assembly Amendment 1, and Assembly Amendment 1, and passed the bill as amended, all on voice votes.

For a full history of the bill, visit the Legislature's bill history page.

AG:ksm