A-Engrossed

Senate Bill 1073

Ordered by the Senate April 10
Including Senate Amendments dated April 10

Sponsored by Senator WOODS

SUMMARY

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure.

Directs State Chief Information Officer to appoint Chief Privacy Officer and describes scope of duties of Chief Privacy Officer.

Directs state agencies to designate agency data officer. Directs Secretary of State**,** [*and*] State Treasurer **and Attorney General** to adopt by rule certain data privacy requirements.

1   **A BILL FOR AN ACT**

2 Relating to data privacy; creating new provisions; and amending ORS 276A.353, 276A.365 and

3   276A.374.

4 **Be It Enacted by the People of the State of Oregon:**

5   <u>SECTION 1.</u> **(1) The State Chief Information Officer shall appoint a Chief Privacy Officer.**

6   **(2) The Chief Privacy Officer shall:**

7   **(a) Conduct a biennial executive department privacy assessment;**

8   **(b) Develop and conduct privacy trainings for state agencies and employees;**

9   **(c) Develop, in coordination with the Chief Data Officer, privacy principles and best**

10 **practices and any necessary statewide policies and guidance for state agencies to implement**

11 **the principles and practices;**

12 **(d) Coordinate data privacy activities with agency data officers designated by state**

13 **agencies pursuant to ORS 276A.365 (1)(g);**

14 **(e) Establish a privacy impact assessment process for information technology initiatives**

15 **involving personally identifiable information;**

16 **(f) Act as a resource for local governments and the public through the dissemination of**

17 **education around the use of personally identifiable information;**

18 **(g) Coordinate with the Chief Data Officer in the integration of privacy principles and**

19 **practices into existing data strategies, programs and plans;**

20 **(h) Otherwise direct, coordinate and oversee state data privacy in accordance with this**

21 **section and other statutes, rules and policies that govern data privacy; and**

22 **(i) Submit a biennial report to a committee or interim committee of the Legislative As-**

23 **sembly related to information management and technology on:**

24 **(A) The status, findings and recommendations that come from a biennial executive de-**

25 **partment privacy assessment conducted under paragraph (a) of this subsection;**

26 **(B) Any updates of the privacy principles and best practices and any necessary statewide**

27 **policies and guidance for state agencies to implement the principles and practices developed**

1 **under paragraph (c) of this subsection; and**

2 **(C) The status of state agency compliance with privacy principles and practices and other**

3 **statutes, rules and policies that govern data privacy.**

4 **(3) The State Chief Information Officer may adopt rules necessary to implement this**

5 **section.**

6 **(4) As used in this section:**

7 **(a) "Executive department" has the meaning given that term in ORS 174.112, except that**

8 **"executive department" does not include:**

9 **(A) The Secretary of State.**

10 **(B) The State Treasurer.**

11 **(C) The Attorney General.**

12 **(b) "State agency" means the executive department.**

13 SECTION 2. ORS 276A.353 is amended to read:

14 276A.353. (1) The State Chief Information Officer shall appoint a Chief Data Officer.

15 (2) The Chief Data Officer shall:

16 (a) Maintain a central web portal for the publication of publishable data under ORS 276A.362.

17 (b) Establish the open data standard as provided in ORS 276A.356.

18 (c) Prepare and publish the technical standards manual as provided in ORS 276A.359.

19 (d) Create an enterprise data inventory that accounts for all datasets used within agency infor-

20 mation systems and that indicates whether each dataset may be made publicly available and if the

21 dataset is currently available to the public. The enterprise data inventory is a public record.

22 (e) **Coordinate with the Chief Privacy Officer to** provide information protection and privacy

23 guidance for state agencies.

24 (f) Establish an enterprise data and information strategy.

25 (g) Identify ways to use and share existing data for business intelligence and predictive analytic

26 opportunities.

27 (h) Identify strategies to combine internal and external data sources.

28 (i) Establish statewide data governance and policy area data governance and provide guidance

29 for agencies about data governance efforts.

30 (j) Oversee the delivery of education and standards to state agencies regarding data quality,

31 master data management and data life cycle management.

32 (k) Form an advisory group to assist the Chief Data Officer in carrying out the duties described

33 in this section and in establishing an enterprise memorandum of understanding for interagency data

34 sharing.

35 (L) Submit a biennial report to a committee or interim committee of the Legislative Assembly

36 related to information management and technology on:

37 (A) The status of agency posting of publishable data; and

38 (B) The status of data sharing within and between agencies, enabling cross-agency analysis to

39 provide information for public purposes, including but not limited to program design and budgeting

40 decisions.

41 (3) The Chief Data Officer may establish and maintain an online forum to solicit feedback from

42 the public and to encourage discussion on the open data standard and publishable data available on

43 the web portal.

44 (4) The State Chief Information Officer may adopt rules necessary to implement ORS 276A.350

45 to 276A.371.

1   **SECTION 3.** ORS 276A.365 is amended to read:

2   276A.365. (1) A state agency shall manage information as a strategic asset throughout the

3 information's life cycle. To improve the management of information resources and reinforce the

4 state's presumption of openness, an agency shall:

5   (a) Collect or create information in a way that supports downstream processing and dissem-

6 ination activities, including:

7   (A) Using machine-readable and open formats;

8   (B) Using data standards approved by the Chief Data Officer in the collection and creation of

9 information in order to promote data interoperability and openness;

10   (C) Ensuring information stewardship through the use of open licenses; and

11   (D) Using common core and extensible metadata.

12   (b) Build information systems to support interoperability and information accessibility.

13   (c) Strengthen data management and release practices to ensure agency data assets are managed

14 and maintained throughout the assets' life cycle by:

15   (A) Adopting effective data asset portfolio management approaches.

16   (B) Creating and maintaining an inventory of agency information resources to be included in the

17 enterprise data inventory.

18   (C) Creating and maintaining a public data listing, including datasets that can be made publicly

19 available but that have not yet been released.

20   (D) Establishing a process to engage with customers and the public to help facilitate and pri-

21 oritize data release.

22   (E) Clarifying roles and responsibilities for promoting efficient and effective data release prac-

23 tices.

24   (d) **Using privacy principles, best practices and guidance developed by the Chief Privacy**

25 **Officer in coordination with the Chief Data Officer,** strengthen measures to ensure that privacy

26 and confidentiality [*are fully protected and that data are properly secured*] **inform data collection,**

27 **governance and management**.

28   (e) Account for the mosaic effect of data aggregation.

29   (f) Incorporate new interoperability and openness requirements into core agency processes.

30   **(g) Designate an employee of the agency to serve as the agency data officer to work in**

31 **consultation with the Chief Data Officer and the Chief Privacy Officer in fulfilling the re-**

32 **quirements of this section.**

33   **(h) Rely on the statewide data management and data privacy policies, rules and guidance**

34 **developed or adopted by the Chief Data Officer and the Chief Privacy Officer.**

35   (2) A state agency shall integrate the following minimum requirements into the project planning

36 documentation and technical design for all new information systems and systems preparing for

37 modernization, as appropriate:

38   (a) System designs must be scalable and flexible and must facilitate the extraction of data in

39 multiple formats, using standards and specifications in the system design that promote industry best

40 practices for data sharing, and separation of data from the application layer to maximize data reuse

41 opportunities;

42   (b) All data outputs of the associated system must meet the requirements described in paragraph

43 (a) of this subsection; and

44   (c) Data schemata and dictionaries must be documented and shared with internal partners and

45 the State Chief Information Officer.

1 (3)(a) A state agency's use of proprietary software may not diminish the ability of the public to

2 inspect and copy a public record.

3 (b) A state agency may not enter into a contract for the creation of a public records database

4 that impairs the ability of the public to inspect or copy the public records of the state agency, in-

5 cluding but not limited to the documentation described in subsection (2)(c) of this section.

6 **SECTION 4.** ORS 276A.374 is amended to read:

7 276A.374. **(1)** The Secretary of State and the State Treasurer shall by rule adopt for each re-

8 spective office requirements related to data that are the same as, or are similar to, the requirements

9 established by ORS 276A.350 to 276A.371 and by rules adopted by the State Chief Information Offi-

10 cer or the Chief Data Officer under ORS 276A.350 to 276A.371.

11 **(2) The Secretary of State, the State Treasurer and the Attorney General shall by rule**

12 **adopt for each respective office requirements related to data privacy that are the same as,**

13 **or are similar to, the requirements established by section 1 of this 2023 Act and by rules**

14 **adopted by the State Chief Information Officer under section 1 of this 2023 Act.**

15 ————————