A BILL FOR AN ACT

Relating to data privacy; creating new provisions; and amending ORS 276A.353, 276A.365 and 276A.374.

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

SECTION 1. (1) The State Chief Information Officer shall appoint a Chief Privacy Officer.

(2) The Chief Privacy Officer shall:

(a) Conduct a biennial executive department privacy assessment;

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

(c) Develop, in coordination with the Chief Data Officer, privacy principles and best practices and any necessary statewide policies and guidance for state agencies to implement the principles and practices;

(d) Coordinate data privacy activities with agency data officers designated by state agencies pursuant to ORS 276A.365 (1)(g);

(e) Establish a privacy impact assessment process for information technology initiatives involving personally identifiable information;

(f) Act as a resource for local governments and the public through the dissemination of education around the use of personally identifiable information;

(g) Coordinate with the Chief Data Officer in the integration of privacy principles and practices into existing data strategies, programs and plans;

(h) Otherwise direct, coordinate and oversee state data privacy in accordance with this section and other statutes, rules and policies that govern data privacy; and

(i) Submit a biennial report to a committee or interim committee of the Legislative Assembly related to information management and technology on:

(A) The status, findings and recommendations that come from a biennial executive department privacy assessment conducted under paragraph (a) of this subsection;

(B) Any updates of the privacy principles and best practices and any necessary statewide policies and guidance for state agencies to implement the principles and practices developed

NOTE: Matter in boldfaced type in an amended section is new; matter [italic and bracketed] is existing law to be omitted. New sections are in boldfaced type.
under paragraph (c) of this subsection; and

(C) The status of state agency compliance with privacy principles and practices and other
statutes, rules and policies that govern data privacy.

(3) The State Chief Information Officer may adopt rules necessary to implement this
section.

(4) As used in this section:

(a) “Executive department” has the meaning given that term in ORS 174.112, except that
“executive department” does not include:

(A) The Secretary of State.

(B) The State Treasurer.

(C) The Attorney General.

(b) “State agency” means the executive department.

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

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

(2) The Chief Data Officer shall:

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

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

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

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

mation systems and that indicates whether each dataset may be made publicly available and if the
dataset is currently available to the public. The enterprise data inventory is a public record.

(e) Coordinate with the Chief Privacy Officer to

provide information protection and privacy
guidance for state agencies.

(f) Establish an enterprise data and information strategy.

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

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

(i) Establish statewide data governance and policy area data governance and provide guidance
for agencies about data governance efforts.

(j) Oversee the delivery of education and standards to state agencies regarding data quality,
master data management and data life cycle management.

(k) Form an advisory group to assist the Chief Data Officer in carrying out the duties described
in this section and in establishing an enterprise memorandum of understanding for interagency data
sharing.

(L) Submit a biennial report to a committee or interim committee of the Legislative Assembly
related to information management and technology on:

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

(B) The status of data sharing within and between agencies, enabling cross-agency analysis to
provide information for public purposes, including but not limited to program design and budgeting
decisions.

(3) The Chief Data Officer may establish and maintain an online forum to solicit feedback from
the public and to encourage discussion on the open data standard and publishable data available on
the web portal.

(4) The State Chief Information Officer may adopt rules necessary to implement ORS 276A.350
to 276A.371.
SECTION 3. ORS 276A.365 is amended to read:

276A.365. (1) A state agency shall manage information as a strategic asset throughout the information’s life cycle. To improve the management of information resources and reinforce the state’s presumption of openness, an agency shall:

(a) Collect or create information in a way that supports downstream processing and dissemination activities, including:

(A) Using machine-readable and open formats;

(B) Using data standards approved by the Chief Data Officer in the collection and creation of information in order to promote data interoperability and openness;

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

(D) Using common core and extensible metadata.

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

(c) Strengthen data management and release practices to ensure agency data assets are managed and maintained throughout the assets’ life cycle by:

(A) Adopting effective data asset portfolio management approaches.

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

(C) Creating and maintaining a public data listing, including datasets that can be made publicly available but that have not yet been released.

(D) Establishing a process to engage with customers and the public to help facilitate and prioritize data release.

(E) Clarifying roles and responsibilities for promoting efficient and effective data release practices.

(d) Using privacy principles, best practices and guidance developed by the Chief Privacy Officer in coordination with the Chief Data Officer, strengthen measures to ensure that privacy and confidentiality [are fully protected and that data are properly secured] inform data collection, governance and management.

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

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

(g) Designate an employee of the agency to serve as the agency data officer to work in consultation with the Chief Data Officer and the Chief Privacy Officer in fulfilling the requirements of this section.

(h) Rely on the statewide data management and data privacy policies, rules and guidance developed or adopted by the Chief Data Officer and the Chief Privacy Officer.

(2) A state agency shall integrate the following minimum requirements into the project planning documentation and technical design for all new information systems and systems preparing for modernization, as appropriate:

(a) System designs must be scalable and flexible and must facilitate the extraction of data in multiple formats, using standards and specifications in the system design that promote industry best practices for data sharing, and separation of data from the application layer to maximize data reuse opportunities;

(b) All data outputs of the associated system must meet the requirements described in paragraph (a) of this subsection; and

(c) Data schemata and dictionaries must be documented and shared with internal partners and the State Chief Information Officer.
(3)(a) A state agency's use of proprietary software may not diminish the ability of the public to inspect and copy a public record.

(b) A state agency may not enter into a contract for the creation of a public records database that impairs the ability of the public to inspect or copy the public records of the state agency, including but not limited to the documentation described in subsection (2)(c) of this section.

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

276A.374. (1) The Secretary of State and the State Treasurer shall by rule adopt for each respective office requirements related to data that are the same as, or are similar to, the requirements established by ORS 276A.350 to 276A.371 and by rules adopted by the State Chief Information Officer or the Chief Data Officer under ORS 276A.350 to 276A.371.

(2) The Secretary of State, the State Treasurer and the Attorney General shall by rule adopt for each respective office requirements related to data privacy that are the same as, or are similar to, the requirements established by section 1 of this 2023 Act and by rules adopted by the State Chief Information Officer under section 1 of this 2023 Act.