SmartSuite

Framework / Privacy / Global Privacy Regulations

Oregon Consumer Information Protection Act, ORS 646A.600 to 646A.628

The Oregon Consumer Information Protection Act (ORS 646A.600 to 646A.628) requires covered entities and vendors to keep reasonable safeguards and to give breach notice within 45 days.



What it is

The Oregon Consumer Information Protection Act, ORS 646A.600 to 646A.628, is the state law that requires any covered entity or vendor that possesses personal information about an Oregon resident to keep reasonable safeguards for it (ORS 646A.622) and to notify affected consumers, and the Attorney General when more than 250 are affected, within 45 days of discovering a breach of security (ORS 646A.604); the act dates from Oregon Laws 2007, chapter 759, and its current text has applied since January 1, 2020 under Senate Bill 684 (Oregon Laws 2019, chapter 180).

At a glance

PUBLISHER
Oregon Legislative Assembly; enforced by the Oregon Attorney General (unlawful practice under ORS 646.607) and the Director of the Department of Consumer and Business Services (ORS 646A.624)

TYPE
Regulation

VERSION
ORS 646A.600 to 646A.628 (Oregon Laws 2007, chapter 759), as amended 2015, 2018 and 2019 (SB 684, Oregon Laws 2019, chapter 180); 2025 edition of the ORS

EFFECTIVE
January 1, 2020 (current text under SB 684); original act 2007

DOMAIN
Privacy

FAMILY
Global Privacy Regulations

REGION
Oregon

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: oregonlegislature.gov/bills_laws/ors/ors646A.html

Why it matters

- **A 45-day consumer notice** Notice goes to each affected consumer in the most expeditious manner possible, without unreasonable delay and not later than 45 days after discovery or notification, delayed only on a law enforcement agency's written request (ORS 646A.604(3)).
- **Attorney General and credit bureau notices** The Attorney General is notified when more than 250 consumers must be told, and nationwide consumer reporting agencies when more than 1,000 are affected (ORS 646A.604(1)(b), (6)).
- **Vendor duties in the statute** A vendor notifies the covered entity within ten days of discovering a breach and notifies the Attorney General itself when more than 250 consumers, or an undeterminable number, are involved (ORS 646A.604(2)).
- **A safeguards program the statute describes** ORS 646A.622(2)(d) lists the administrative, technical and physical safeguards that satisfy the duty, from a designated coordinator and patch management to destruction of records at disposal.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Oregon ORS 646A

ORS 646A.622 Safeguards Library

Load the listed safeguards (seven administrative, four technical, four physical) as requirements with owners, status and evidence, or record the GLBA, HIPAA or stricter-law basis relied on under subsection (2).

Personal Information Inventory

Track where each element of personal information under ORS 646A.602(12) is held, including elements that count without a name, so the scope and type of information for a notice can be read from the system, in Privacy Management.

Risk Assessment and Patch Management

Run the regular risk identification, safeguard assessment and user access review in subsection (2)(d)(A), and the security update and patch management program in (2)(d)(B), as recurring records.

Vendor Contracts and Ten-Day Notice

Track each vendor that holds personal information, the contract clause required by (2)(d)(A)(v) and the vendor's ORS 646A.604(2) duty to notify within ten days, in Third Party Risk Management.

Breach Notice Workflow

Run discovery date, the reasonable measures in ORS 646A.604(3)(b), the 45-day deadline, law enforcement delay requests, notice method and the six required contents, and the subsection (8) no-harm determination with its five-year retention.

Attorney General and Credit Bureau Reporting

Record the Attorney General notice and sample copy above 250 consumers, the nationwide consumer reporting agency notice above 1,000 with any police report number, and the disposal records required by (2)(d)(C)(iv).

Common framework mappings

CIS Controls v8.1 · GDPR · GLBA Safeguards Rule (16 CFR Part 314) · ISO 27001:2022 · ISO 27701 · NIST CSF 2.0 · NIST Privacy Framework v1.0 · NIST 800-53 Rev.5 · PCI DSS 4.0.1 · SOC 2

Official resources

Oregon Revised Statutes (ORS) 646A - Consumer Information Protection Act

Provides the official legal text of Oregon's consumer information protection regulations.

oregonlegislature.gov/bills_laws/ors/ors646A.html

Frequently asked questions

Who must comply with the Oregon Consumer Information Protection Act?

Any covered entity, meaning a person that owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information about an Oregon resident in the course of business, vocation, occupation or volunteer activities, and any vendor that holds such information under contract to a covered entity (ORS 646A.602(5), (19)). Person includes individuals, companies, nonprofits and public bodies (ORS 646A.602(11)). Both covered entities and vendors carry the safeguards duty in ORS 646A.622, and each has its own notice duty in ORS 646A.604.

What is personal information under ORS 646A.602?

A consumer's first name or initial and last name combined with a Social Security number, a driver license or state identification card number, a passport or other United States identification number, a financial account or credit or debit card number with any required code or other information that would permit access, biometric data used to authenticate identity, a health insurance policy or subscriber number, or information about medical history, condition, diagnosis or treatment; or a user name or other account identifier with the means to authenticate it; or any of those data elements without the name if they are not encrypted or redacted and would enable identity theft (ORS 646A.602(12)). Lawfully public government-record information other than a Social Security number is excluded.

 © 2026 SmartSuite Inc. All rights reserved.

How quickly must a breach be reported in Oregon, and to whom?

A covered entity notifies each affected consumer in the most expeditious manner possible, without unreasonable delay and not later than 45 days after discovering or receiving notification of the breach, delayed only on a law enforcement agency's written request (ORS 646A.604(3)). If more than 250 consumers must be notified, the Attorney General is notified as well (646A.604(1)(b)), and if more than 1,000 are affected, the nationwide consumer reporting agencies (646A.604(6)). A vendor notifies the covered entity as soon as practicable and not later than ten days after discovery, and notifies the Attorney General itself above 250 consumers unless the covered entity has (646A.604(2)).

What safeguards does ORS 646A.622 require?

Covered entities and vendors must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information, including at disposal (ORS 646A.622(1)). They comply by following a stricter state or federal law, Gramm-Leach-Bliley Act Title V regulations or the HIPAA and HITECH rules, or by an information security program with administrative safeguards (a coordinator, regular risk identification, safeguard assessment, training, service providers bound by contract, program adjustment, review of user access privileges), technical safeguards (network and software risk assessment, security updates and patch management, monitoring and response to attacks, testing of key controls) and physical safeguards (collection-to-disposal risk assessment, intrusion response, life-cycle protection, and disposal by burning, pulverizing, shredding or modifying records and destroying or erasing media) (646A.622(2)). Small businesses meet a scaled standard (646A.622(5)).

What are the penalties for violating the act?

A violation of any provision of ORS 646A.600 to 646A.628 is an unlawful practice under ORS 646.607, enforced by the Attorney General (ORS 646A.604(11)(a)). In addition, the Director of the Department of Consumer and Business Services may investigate, subpoena records, issue cease-and-desist orders, order compensation to injured consumers and impose a penalty of not more than $1,000 for every violation, with each day of a continuing violation a separate violation and a maximum of $500,000 for any occurrence (ORS 646A.624(3), (4)). The remedies are cumulative with any others available under law (646A.604(11)(c)).

License included / downloadable: Yes ORS chapter 646A and the enrolled SB 684 are Oregon state law, published free by the Oregon Legislative Assembly; the platform links to the official texts.

Full framework page and mappings: smartsuite.com/frameworks/us-oregon-ors-646a-consumer-information-protection-act

 © 2026 SmartSuite Inc. All rights reserved.