Oregon Department of Justice

Oregon Consumer Privacy Act

Data Protection Assessment Guidelines for Businesses

What is a Data Protection Assessment?

This is an internal document your company or non-profit must generate when you are processing (maintaining, storing, collecting, sharing, modifying) certain types of consumer data. This does not get posted publicly but represents your company's good faith decision-making regarding the Oregon Consumer Privacy Act. If there is a consumer complaint filed, or evidence of wrongdoing regarding consumer privacy, your company could be asked to provide this document to the Attorney General's office. It is otherwise confidential![1]

When does my company need a Data Protection Assessment?

Anytime data processing represents a heightened risk to consumers.[2] What does that mean? Let's break it down into data types.

1. Heightened risk activities for **Personal Data** (identifies a person, a device linked to a person):
    a. Are you processing it for targeted advertising?
    b. Are you selling Personal Data to third parties?
    c. Are you processing the Personal Data for profiling that may result in unfair treatment, intrusion, or harm (physical, emotional, etc.)?
2. Heightened risk activities for **Sensitive Data** (identifies a sensitive aspect of an individual, ex: health **OR** data for children under 13):
    a. Are you processing sensitive data?

If you answered "yes" to these questions, your company's data collection likely represents a heighted risk to consumers. This isn't illegal, but your company needs to conduct a Data Protection Assessment and keep it on file for **five years**.

How many Data Protection Assessments does my company need?

You can explain similar data decisions of the same level or type of "harm" together. For example, your company doesn't need a separate assessment every time it sells Personal Data to third parties, as long as all of those sales are treated similarly as outlined by a singular Data Protection Assessment.

**Most states allow you to use the same Data Protection Assessments to meet different state laws. These guidelines are written based off Oregon law. An assessment done to comply with another law can satisfy OCPA requirements as long as it reasonably similar to these Data Protection Assessment guidelines.*

---

[1] *See* ORS 646A.586(7) (data protection assessment confidentiality).

[2] *See* ORS 646A.586(1) (data protection assessment for processing activities with heightened risk of harm).

What should my Data Protection Assessment cover?

There is not a set form your company must fill out. We have provided some non-exhaustive suggestions/guidelines. Every company or non-profit has unique factors to consider, so focus on the *intent* behind these suggestions. The depth, level of detail, and scope of your assessment should reflect the risk presented, size of the company, and potential impact to consumers.

This Oregon law is **not retroactive. Data Protection Assessments only apply to data processing activities done on or after July 1, 2024 (July 1, 2025 for non-profits).*[3]

Checklist to Consider/Address:

1. **Need:** Explain broadly what your data collection hopes to achieve. Summarize why your company needs this Data Protection Assessment. *Note: You can include supportive documentation, such as a new project or marketing proposal.*[4]
2. **Benefit:** How does processing Personal or Sensitive Data directly or indirectly benefit your company, stakeholders, consumers, and the public? What is the intended effect on individuals?[5]
3. **Nature:** What is the nature of the data your company is processing? How will it be collected, used, stored, and/or deleted? Roughly how many individuals will be affected and where do they live? Will your company be sharing the data with anyone? If so, who? *Note*: *It might be helpful to create a flow diagram or other representation of data flow.*[6]
4. **Risk:** How might the processing of Personal or Sensitive Data pose risks to consumers?[7]
    a. What safeguards does/will the company take to minimize this risk?
5. **Proportionality:** Can my company collect *less* Personal or Sensitive Data and instead rely on Deidentified Data (data that can't be linked to individuals) to reach the same goals? If so, implement changes and document them![8]
6. **Context:** What reasonable expectations might consumers have about how you're using this data? *Your processing of data should match what is outlined in the company Privacy Policy when the data was gathered, unless you have obtained consent to expand your use of the data.* What have consumers actually agreed to?[9]

---

[3] *See* ORS 646A.586(5) (operative date).

[4] *See* ORS 646A.572(6) and (7) (scope; exclusions); ORS 646A.586(1) (data protection assessment for processing activities with heightened risk of harm).

[5] *See* ORS 646A.586(2) (benefits weighed against risks)

[6] *See* ORS 646A.572(6) (nature and purpose of collection, use or retention); ORS 646A.586(1) and (2) (activities with heightened risk of harm; benefits weighed against risks)

[7] *See* ORS 646A.578(1)(c) (safeguards); ORS 646A.586(2) (benefits weighed against risks)

[8] *See* ORS 646A.578(1)(b) (data minimization); ORS 646A.583 (deidentified data).

[9] *See* ORS 646A.578(1)(a) and (b) (privacy notice); ORS 646A(2) (prohibition on expansion of processing as set out in privacy notice without consent); ORS 646A.574(3)(L) (consumer's reasonable expectations).

a. What is the context for how this data is gathered? Was it an explicit opt-in, required for account registration, etc.? Would they expect you to use their data in this way?

b. What is the relationship between the company and consumer? Is it a close, consistent relationship model? Is there a power differential between consumer and company?

7. **Records:** Make sure your internal record-keeping is thorough. Who discussed/wrote this document? When was it written and when was it updated? Who signed off on each version? Are there actionable items that need to be addressed and did that happen? The more “eyes” on this, the better for your company! Data privacy decisions should not just be made by one person, in isolation from the rest of the company.

Disclaimer: This document is for informational purposes only, and does not implement, interpret, or make specific the law enforced or administered by the OCPA, establish substantive policy or rights, or constitute legal advice. It presents some general guidelines for compliance. Make sure to engage with and read the full statutory language.