Oregon Department of Justice
Office of the Attorney General

ELLEN F. ROSENBLUM
Attorney General

LISA UDLAND
Deputy Attorney General

Oregon Consumer Privacy Act – SB 619

Background:

In recent years, consumers, advocates, and policymakers across the country have become increasingly concerned about the vast amount of data collected by companies and how consumer information is used. Consumer data has immense value – it can fuel innovation and help serve the needs and desires of customers and clients. But our data can also be used to target, exploit and expose consumers in harmful and sometimes dangerous ways. We need a system to rebalance this power disparity and give consumers more knowledge and control over their privacy.

In June of 2019, the Attorney General convened a Consumer Privacy Task Force to answer the growing call for comprehensive state consumer privacy legislation. Since that time the Task Force has grown from about 30 to more than 150 participants from a wide variety of sectors and perspectives. The goal of this task force was to develop a comprehensive consumer privacy framework to provide Oregonians with basic rights and more control over their data privacy. Many other states have proposed - and some have passed – their own state privacy laws. They include California, Virginia, Colorado, Utah, Washington and Connecticut.

The Task Force has been working for several years on Oregon-specific privacy legislation, using the basic framework that most states have adopted to develop a bill that provides meaningful protections consumers and is workable for industry.

Proposal:

The Oregon Consumer Privacy Act will affirmatively provide Oregonians with a number of important rights over their personal information, and imposes specific obligations on businesses who collect, use, store, disclose, analyze, delete or modify (“process”) consumers’ personal data (“controllers”) and those entities who process personal data on behalf of controllers (“processors”):

- **Right to Know:** Consumers will have the right to know whether controllers are processing their data, as well as the categories of data being processed and third parties the data has been disclosed to. Consumers will also have a right to obtain a copy of the consumer’s personal data that a controller has or is processing;

- **Right to Correction:** Consumers will have the right to correct inaccuracies in their data;
- **Right to Deletion:** Consumers will have the right to require a controller to delete their personal data held by a controller;
- **Right to Opt Out:** Consumers will have the right to opt out of the processing of their personal data for targeted advertising, sale or profiling of the consumer in a way that produces legal effects; and
- **Right to Data Portability:** When consumers exercise their right to obtain a copy of their personal data held by a controller, it must be provided in a portable and useable format.

The Act contains heightened protections (a requirement that data may not be processed without a consumer's affirmative "opt in" consent) for "sensitive data", which includes:

- Personal data revealing racial or ethnic background, national origin, religious beliefs, mental or physical condition or diagnosis, sexual orientation, gender identity, crime victim status, or citizenship or immigration status;
- Genetic or biometric data; and
- Precise geolocation data.

Children and youth are also given heightened protections under the Act. Controllers must follow the requirements of the federal Children's Online Privacy Protection Act (COPPA) when processing data of children under 13 years old. Further, "opt in" consent is required for targeted advertising or sale of the personal data of a youth 13 to 15 years old.

The Act requires controllers to provide a comprehensive privacy notice, including:

- Categories of data processed;
- Purposes for processing data;
- How to exercise consumer rights;
- Categories of data shared with third parties and categories of third parties receiving data; and
- Contact information.

Controllers must also:

- Limit the collection of personal data to what is adequate, relevant and reasonably necessary for the purposes set out in the controller's privacy notice;

- Obtain consent to process data beyond the specified purposes set out in the privacy notice;
- Maintain reasonable data security practices;
- Not discriminate against consumers for exercising their rights under the Act (note that there is an exception here for loyalty rewards programs);
- Ensure that deidentified data stays deidentified; and
- Conduct data privacy assessments for activities that present a heightened risk of harm to a consumer, including targeted advertising, sale of data, profiling that presents a risk of unfair treatment, disparate impact or injury, and processing of sensitive data.

To exclude small businesses, the Act has a threshold that must be met before it applies. To be subject to the Act, a business must annually control or process personal data of:

- ≥100,000 consumers and/or devices linked to consumers; or
- ≥25,000 consumers, while deriving ≥25% gross revenue from personal data sales.

As with any comprehensive regulatory policy, the Privacy Act includes certain exemptions to appropriately limit its scope and avoid conflict with other legal obligations and practical considerations. These exemptions include:

- Data of persons engaging in commercial activity (operating a business);
- Employee and employer data;
- Public bodies;
- Deidentified data;
- Data already regulated under several federal laws; and
- Compliance with other legal requirements and process, law enforcement, security incident response, technical repairs, providing the requested service, and health and safety.

Contact:

Kimberly McCullough, Legislative Director, 503-931-0418, kimberly.mccullough@doj.state.or.us
Kate Denison, Deputy Legislative Director, 971-599-9851, kate.e.denison@doj.state.or.us