A-6

MODEL PRIVACY POLICY FOR ROAD USAGE CHARGING

WA RUC

WA RUC

Model Privacy Policy for Road Usage Charging

D'ARTAGNAN CONSULTING

CONTENTS

EXECUTIVE SUMMARY

The purpose of this report is to summarize the issue of privacy protection in distance-based road usage charge systems (RUC), explore the major applicable privacy policies and present a model privacy policy for road usage charge systems in the United States.

Background. When a government proposes a public policy initiative that would require the use of personal information and data from a broad expanse of the population, the privacy issue comes to the forefront as a major issue. The idea of collection of a distance-based road usage charge calculated on personal travel data to fund the public road system is just such an initiative.

To obtain the distance-traveled data for an individual vehicle, the owner or lessee of the vehicle must report the required travel data, or in some cases an estimation of such, to a billing entity. The billing entity will apply the reported distance-traveled data to calculate the charge and present the amount to the responsible person (the RUC payer) as an obligation for payment. During the course of assessing the amount owed, various persons and entities related to collection of the distance-based road usage charge will necessarily collect sensitive information and data from responsible persons and their vehicles, including identifiers, financials, mileage totals and travel time and location.

Protection of personal privacy is important to many and some are impassioned about it. In the public survey conducted prior to the launch of the WA RUC pilot in 2017, 20% of respondents identified protection of personal information as the most important issue to them. In the first survey of pilot participants conducted in early 2018, privacy ranked as the top issue, with 83% of respondents characterizing it as “very important” to them.

Legal protections create law-based restrictions or limitations to use of such data for purposes other than collection of the charge. The United States Constitution and state constitutions are not specific about protection of privacy generally and Congress has not enacted a general privacy protection law at the federal level. For any legal certainty about the protection of privacy for a RUC program, state legislatures must enact legislation.

Recommendations. The EU GDPR and the California Consumer Privacy Act offer certain provisions that should improve the protection of personal privacy that Oregon law has in place for RUC. The following provisions should be included in a model privacy policy for Washington’s RUC program.

- **Protection of RUC information from disclosure**. The model privacy policy should protect from disclosure any personal information identifying or nominally related to a RUC payer and should only protect RUC information rather than information not accumulated for the road usage charge system.

- **Responsibility for privacy protection**. The obligation to comply with the model privacy policy falls to whoever holds the information provided there is imposition of adequate oversight.

- **Establishment of specific privacy protections**. The model privacy policy should apply specific requirements, limitations and prohibitions directly related to protection of personal information collected for a road usage charge program and direct service providers and the authorized agency to establish, publish and adhere to an organizational usage and privacy policy available in writing.

- **Exemptions**. The model privacy policy should exempt from the requirement for non-disclosure of personal information persons and entities operating the road usage charge system and facilitating payment to the extent necessary to fulfill their duties. Other exemption should include the RUC payer with regard to his or her own personal information and entities for whom the RUC payer has given express approval to receive specific personal information. A state should consider other exceptions for law enforcement activities with probable cause for use of the personal information.

- **Rights of RUC payer**. A RUC payer should have the right to access, the right to inquire and the right to examine personal information as well as the right to rectify errors or inaccuracies in personal information and the right to erasure of location and metered use data after it is no longer needed following a specified period. Exceptions to erasure may include consent of the RUC payer, retention of anonymized aggregated information used for traffic management and research and monthly summaries of metered use for accounting purposes. At the outset of the engagement, service provider for a road usage charge system should provide road charge payers information of their rights pertaining to personal information and specifically how to exercise them.

- **Exercise of rights**. The specific requirements for responding to a request for exercise of rights—transparency, intelligible, easily accessible, clear and plain

language—should be described in law. A service provider must never refuse a request for exercise of rights.

- **Prohibition from discriminatory behavior**. A model privacy policy should prohibit service providers from engaging in discriminatory behavior against RUC payers for exercising their rights. A service provider may offer a different price to RUC payers for services as long as the price is directly related to the value provided.

- **Security measures**. A model privacy policy should require a service provider to implement security measures to protect personal information to a level appropriate to the risk of disclosure.

- **Breaches**. A model privacy policy should require service providers to provide notice to an authorized agency when a breach happens and provide specific information about the nature of the breach and its likely impact. Service providers should provide notice to RUC payers of any breach where the service provider has not implemented appropriate security measures, has not taken subsequent measures to reduce high risk or has not made an effective public communication about the breach.

- **Designate a personal information officer**. The model privacy policy should require a service provider to designate a personal information officer with the responsibility as contact for RUC payers and to ensure compliance.

- **Certification**. The model privacy policy should require an authorized agency to establish certification mechanisms for service providers to demonstrate compliance with the privacy protection provisions. Certification bodies should issue and renew certifications on the basis of criteria set by the authorizing agency.

- **Remedies**. Each state adopting a road usage charge program should adopt an appropriate assortment of remedies to enable aggrieved RUC payers to seek redress for violation of their rights. Each state should determine the precise nature of the set of remedies and the penalty amounts.

- **Record of access**. The model privacy policy should require a service provider to maintain a record of access to personal information the service provider holds.

1 INTRODUCTION

1.1 Purpose and Context

The purpose of this report is to summarize the issue of privacy protection in distance-based road usage charge (RUC) systems, explore the major applicable privacy policies, and present a model privacy policy for RUC systems in Washington.

The desire for privacy is personal. Privacy expectations vary depending on the individual and the circumstance. Some have no concern for their personal privacy while others demand protection of complete anonymity.

When a government proposes public policy requiring the use of personal information and data from a broad expanse of the population, the privacy issue comes to the forefront as a major issue. The idea of collection of a distance-based RUC calculated on personal travel data to fund the public road system is just such a proposal.

The importance of privacy also depends upon policy applications. For example, while in most cases automobile travel is a personal endeavor with little government involvement other than obedience to traffic laws, commercial trucking is a regulated industry with driving hour limits, rest requirements, and safety rules with drivers familiar with behavior oversight. Privacy expectations under a RUC system will vary accordingly whether the owner of the vehicle is a private citizen versus a commercial trucking company.

1.2 Objectives

The objectives of this paper are as follows:

- Explain the general public's preferences for a privacy law covering an enacted distance-based RUC.
- Present and analyze earlier efforts to address privacy in the context of a distance-based RUC.
- Describe adopted privacy protection policies and law in the context of a distance-based RUC.
- Analyze recently enacted general privacy laws in the European Union and the State of California for additional advisable polices for inclusion in a model privacy policy.

- Discuss the key issues pertaining to privacy protection in the context of a distance-based RUC.
- Present the model privacy policy.

2 BACKGROUND

2.1 What is privacy protection in the context of a RUC program?

A distance-based RUC system is necessarily based on data directly related to measurement of the length of individual vehicle travel during a specific time period. In the United States, the unit of measurement used for this purpose is the mile; in Europe, Australia, New Zealand, Canada and many other parts of the world, the unit of measurement for this purpose is the kilometer.

To obtain the distance-traveled data for an individual vehicle, the person responsible for the vehicle (owner, lessee, or operator) must report the required travel data, or in some cases an estimation of such, to a billing entity. The billing entity will apply the reported distance-traveled data to calculate a fee, tax or charge and present the amount to the responsible person as an obligation for payment.

In assessing the amount owed, various persons and entities related to collection of the distance-based RUC will necessarily collect sensitive information and data from responsible persons and their vehicles. The information and data collected may include identifying information, financial information, distance-traveled totals, travel times, and locations.

The RUC system can protect the processing of sensitive information and data in two ways: technically and legally. Technical protections can reduce or eliminate development or access to some data used in collection of a road usage charge. Legal protections create law-based restrictions or limitations to use of such data for purposes other than collection of the charge and impose fines or other enforcement consequences for violations.

The privacy issue for collection of distance charges was not a major issue while the idea was mere theory. The use of GPS technology in pilot tests, however, raised suspicions[1]. Negative public reactions to the first distance charge pilot test revealed that a technology-

[1] Appendix A describes a history of the privacy issue in early RUC investigations.

solution alone would not mollify generally held privacy concerns over use of GPS data[2]. The emphasis shifted away from a technology solution to administrative and legal solutions[3].

To this day, public concerns about RUC often center on privacy, including in Washington. In the public survey conducted prior to the launch of the WA RUC pilot in 2017, 20% of respondents identified protection of personal information as the most important issue to them. In the first survey of pilot participants conducted in early 2018, privacy ranked as the top issue, with 83% of respondents characterizing it as “very important” to them.

2.2 Data and information accessed and used in a RUC program

There are nine essential functions for operating a RUC system.

- Identify the vehicle subject to the program
- Identify the owner or lessee of the vehicle subject to the program
- Calculate distance driven during a specific time period
- Assign distance traveled allotments to various geographic locations, if the program requires it
- Access the travel data
- Apply road usage charge rates to the data
- Present a billing to the payer of the charge
- Collect payment
- Enforce payment

To perform each of the essential functions, the system must acquire particular information and data. Among the data accessed and acquired includes the following.

- Vehicle registration plate number
- Vehicle identification number (VIN)
- Name of owner or lessee of the vehicle
- Access information of owner or lessee of the vehicle (address, email address, telephone number)

[2] Recent experiments with Blockchain may have begun to change the view of the general public with regard to protection of sensitive data. Application of the decentralized nature of Blockchain to a RUC system, however, is not even in its infancy.
[3] For a more thorough discussion of the development of privacy protection in RUC systems and programs, see Appendix C.

- Distance traveled data, which may include one or more of the following:
  - Periodic odometer readings
  - Metered use of data by latitude and longitude or summaries of the same
  - Travel pattern data
- Travel data record
- Billing and payment record
- Payment information, which may include:
  - Bank account information
  - Credit card number
- Enforcement record

The administrator or service provider for a RUC system will also acquire other personal information merely by participation in the program:

- RUC account identification number
- Identification code for the mileage meter installed in the vehicle

All of this information can identify a person and the person's behavior. As such, this information should be considered sensitive and protected as personal information subject to the Model Privacy Policy.

2.3 The legal basis for privacy protection in the United States

The United States does not have any general privacy protection law at the federal level except for an inference in the U.S. Constitution stated in case law of the Supreme Court determined on a case-by-case basis. Residents of a state cannot rely upon Supreme Court case law to understand how information and data obtained during collection of a RUC will be protected. For specificity and assurance of privacy protections in a RUC system, a state legislature or Congress must enact a statute.

Without federal direction on general protection of privacy data and information, policy enactments protecting privacy for road usage charge data must come from the states. According to the National Conference of State Legislatures, only ten states (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, Washington) have privacy protection provisions in their state constitutions. These constitutional provisions apply to government action but not necessarily private actions.

For legal certainty about the protection of privacy, state legislatures must enact legislation[4].

2.4 Recent privacy law enactments

Recently, the California Legislative Assembly enacted the California Consumer Privacy Act which primarily focuses on imposing requirements on businesses and rights to consumers with respect to consumer data rather than restricting or directing the actions of government. The European Union implemented the General Data Protection Regulation (GDPR) earlier this year with the stated purposes of protecting fundamental rights and freedoms of natural persons regarding the processing of their personal data and their right to protection of personal data, and free movement of personal data within the European Union. The comprehensiveness and reach of the EU's GDPR and the California privacy law renders them relevant for consideration in development of a model privacy policy framework for distance charging in the United States[5].

[4] For a more information on the legal basis for privacy protection in the United States, see Appendices B and D.
[5] For a more information on the European Union's General Data Protection Regulations, see Appendix D.

3 THE CENTRAL ISSUES FOR A MODEL PRIVACY POLICY

3.1 Heavy versus light vehicles

While some privacy issues for operators and owners of heavy and light vehicles may be similar—such as integrity and accuracy of the data, responding to requests for exercise of rights, nondisclosure of personal information and security—concerns about government access to vehicle location and travel patterns tend to be less of a concern for heavy vehicles because commercial traffic is a regulated industry with minimal expectations for personal privacy. Accordingly, a model privacy policy for light vehicles, where the expectations of privacy are higher, may be more stringent than a privacy policy for heavy vehicles.

The model privacy policy for light vehicles is presented in section 8. A model privacy policy for heavy vehicles is not presented in this paper.

3.2 Central issues

The central issues for structuring the model privacy policy were determined through cross-analysis of three privacy laws of relevant to its development: the European Union's General Data Protection Regulation (2018), the California Consumer Privacy Act of 2018, and the privacy protection provisions of the Oregon Road Usage Charge Program (OReGO), the only light vehicle privacy protection statute enacted into law.

3.2.1 Fundamentals: purpose, protected information, material scope, territorial scope

3.2.1.1 Stated purpose

The purpose of the model privacy policy will establish a central focus. It should directly relate to the essential function of the program for which the privacy policy is developed; that is protection of personal information of those participating in a RUC program.

For this purpose, personal information should identify a person or relate to a person in a way necessary for collection of travel data or payment of a RUC.

Recommendation: The model privacy policy should protect personal information collected under a RUC program from disclosure.

3.2.1.2 Definition of personal information: What is protected from disclosure?

The model privacy policy should protect from disclosure information identifying or nominally related to a person. Should the definition of personal information, however, include anonymized information collected from a RUC payer after a service provider has anonymized it? Information that comes from or relates to a person, even if the person can no longer be identified or related to it, could be treated as personal information. Such information should hold the status as a property right even though the owner is no longer apparent. The policy basis for protection of anonymized information is unclear.

In creating an exception from treating anonymized information as personal information, it may prove necessary to condition such an exception upon a service provider's implementation of technical safeguards and processes that prohibit re-identification or prevention of inadvertent release of the information. Otherwise, information that is anonymized may not stay that way thus undercutting any purpose for the exemption.

Recommendation: The model privacy policy should protect from disclosure any information identifying or nominally related to a RUC payer. There should be an exception for anonymized information provided the exception is conditioned upon the authorized agency or a service provider implementing technical safeguards and processes that prohibit re-identification or prevention of inadvertent release of the information.

3.2.1.3 Material scope: Which information should be protected under a model privacy policy?

The essential purpose of a RUC system is to collect travel data related to a particular vehicle to enable application of a charge rate to determine the charges due for a period of time. The system will also collect identifying information to associate the vehicle with its owner or lessee and financial information provided by the RUC payer to enable payment. This RUC information is necessary for the RUC program to collect; therefore, all of it should be considered personal information subject to the specific requirements, limitations, and prohibitions of a model privacy policy.

The question remains whether information collected beyond RUC information by a service provider should also be subject to the model privacy policy for a RUC program. This would include information used by the service provider to apply value-added services upon the request of a subject vehicle owner or lessee (RUC payer). The typical data used for value-added services will come from vehicle information accessed through the OBD-II port or other telematics. This may include driving behavior (speed, hard braking), maintenance (battery life, pollution control devices), travel location (ring fencing), among other vehicle and travel information.

Requiring a service provider to protect information acquired other than for the purpose of collecting a RUC will increase the cost of collection and impede formation of a private sector market in an account-based, open system. Reducing the operating costs to an affordable level is one of the principal challenges of implementing a RUC program into law. Taking advantage of an open, competitive market will put downward pressure on operating costs. Therefore, adding cost items or disadvantaging formation of an open market for RUC should be avoided unless it is part of a broader social policy applied to all businesses collecting online data.

Enactment of legislation applying a model privacy policy to “other than RUC” information should prove difficult politically. In the United States, only the state of California has enacted a broad-ranged privacy protection law for online, consumer data. Protecting the privacy of only RUC information should prove much easier to enact since broader societal issues would not come forward into the debate.

Recommendation: The model privacy policy should only protect RUC information.

3.2.1.4 Territorial scope: Who should protect personal information, the government or whoever holds the information?

In a RUC system, all elements of the data and RUC collection process flow from actions undertaken by the authorized agency. Forming an open market for collection of RUC will require the affirmation and actions of the authorized agency designated the responsibility to collect RUC in the authorizing legislation. The authorized agency will initiate and operate the procurement process for attracting and engaging service providers. With such authority, the authorized agency could impose its obligation to protect RUC information onto service providers as part of the contractual arrangement to perform services for the RUC program.

Alternatively, the model privacy policy could apply directly to RUC service providers alone and not the authorized agency. This is the approach undertaken in the European Union, California and Oregon laws. Such an approach requires adequate oversight and enforcement capabilities and all three laws do albeit differently.

Recommendation: The obligation to comply with the model privacy policy falls to whoever holds the information provided there is imposition of adequate oversight.

3.2.2 The basics: responsible agency, nature of protection, public records

3.2.2.1 Identifying the responsible agency

Whether a state adopting a RUC program authorizes an existing agency as the authorized agency to enforce protection of personal information accessed for the program or creates a new agency for this purpose will be determined by the traditions and culture for governmental institutions in that state. Examples of an existing agency charged with this responsibility include a department of transportation (per ORe*GO*), vehicle registry agency, or a department of revenue. Creating a new agency for this purpose would have the advantage of establishment of a new agency culture around privacy protection but this outcome will likely depend upon the size of the program at the outset.

Recommendation: Designate an existing agency as the authorized agency responsible for protecting personal information in a RUC program.

3.2.2.2 Whether the authorized agency can operate as a service provider

While it is not necessary for a government agency to provide RUC services similar to a service provider certified to provide the same services, a state may prefer to have a government option to collect RUC and data rather than have only an open commercial market available for these services. Oregon's RUC Program (ORe*GO*) is just such a program. California tested only an open commercial market in its pilot tests, and Washington is following suit. Opinions vary on this point. The model privacy policy allows for the option to go either way.

Recommendation: Appoint a state government agency to engage in road usage charge collection services similar to those provided by a service provider so that a RUC payer may have the choice of either collection of road usage charges by a contracted service provider or a government agency.

3.2.2.3 Nature of protection

A service provider of services related to collection of travel information and collection of a RUC from payers must have a designated responsibility to comply with a model privacy protection policy. In establishing Oregon's RUC program, the legislature applied specific requirements, limitations, and prohibitions directly related to protection of personal information collected for the program. In the Model California Road Charge Privacy Legislation, the California Technical Advisory Committee chose to recommend that a service provider and the authorized agency each should have assigned an affirmative public duty to protect the confidentiality of personal information and maintain reasonable security procedures and practices to protect against unauthorized access.

These two approaches can equally accomplish the same protection but interpretation of each will yield distinct results. The specificity of the Oregon approach can offer greater certainty to service providers and authorized agencies while the California approach offers a way for protection to grow as new situations arise.

Either way, the model privacy policy could direct service providers and the authorized agency to establish, publish and adhere to an organizational usage and privacy policy available in writing. While this is an added burden to the service providers and the authorize agency, establishing such a policy and committing to its application will put the privacy issue strongly before these entities with greater likelihood of adherence.

Recommendation: The model privacy policy should apply specific requirements, limitations and prohibitions directly related to protection of personal information collected for a RUC program and direct service providers and the authorized agency to establish, publish and adhere to an organizational usage and privacy policy available in writing.

3.2.2.4 RUC personal information as a public record

Many states have comprehensive public records laws to ensure transparency for government actions. Transparency for public information, of course, is a policy directly opposed to privacy for public information. There are exemptions to public records laws for certain types of sensitive information obtained by the government. Travel data and identity and financial information are certainly sensitive to most people and an exemption would be in order.

Recommendation: Personal information obtained for purposes of collecting a RUC should be designated a public record under public records laws but exempted from disclosure to protect the privacy of the RUC payer.

3.2.2.5 Exceptions to nondisclosure

Persons and entities necessary to operating the RUC system and facilitating payment must have access to and use personal information to fulfill their duties. The model privacy policy should provide an exception from non-disclosure for those participating in system operations and for the RUC payer. Other potential exceptions may include an entity for whom a RUC payer has given express approval to receive specific personal information and police officers who have a valid court order based on probable cause. A state may find reasonable other exceptions for other law enforcement activities.

Recommendation: The model privacy policy should exempt from the requirement for non-disclosure of personal information persons and entities operating the RUC system and facilitating payment to the extent necessary to fulfill their duties. Other exemption should include the RUC payer with regard to his or her own personal information and entities for whom the RUC payer has given express approval to receive specific personal information. Washington should consider other exceptions for law enforcement activities with probable cause for use of the personal information.

3.2.3 Rights of RUC payers

3.2.3.1 Which rights should a RUC payer have?

Rather than rely entirely on a government watchdog agency for oversight or self-monitored service providers to protect personal information, providing RUC payers certain rights and remedies can add another layer of protection.

First and foremost, an added layer of protection requires that the RUC payer can learn about the personal information held by an authorizing agency or service provider. This compels establishment of a right to access to personal information for RUC payers and to inquire about the nature, accuracy, status and use of their information and the right to examine it.

Should a RUC payer find errors or inaccuracies in the personal information, the RUC payer should have an ability to correct them. A RUC payer with a right to rectification of

errors or inaccuracies in personal information would enable an effective oversight mechanism from those with the best information.

To ensure a service provider cannot retain personal travel information for an unlimited period, RUC payers should have the right to erasure of location or daily metered use data no longer necessary for the purpose for which it was created, provided or accessed. This would include a time limit based on events such as payment, dispute resolution or noncompliance investigation.

If while exercising the right to examine personal information a RUC payer discovers that a service provider has not complied with a requirement to erase location and daily metered use data by mandated deadlines, the RUC payer should be able to demand erasure of that information by their own action.

A service provider should not be able to retain the location and daily metered use data beyond the time limit where the RUC payer consents to retention.

A second exception to erasure may include retention of records accumulated as anonymized aggregated information and used for purposes of traffic management and research. There is a valuable public purpose for transportation planning agencies to have access and use this information provided the information is managed in a way that there is no ability to identify individual RUC payers.

A third exception to erasure may include monthly summaries of metered use of subject vehicles but not location information. With specific travel information removed, these monthly summaries are necessary for proper accounting of the RUC accounts of RUC payers.

Finally, a state may decide that the obligation for erasure should not apply to the extent the location and daily metered use data is necessary to comply with legal obligations or actions taken with regard to legal claims.

A RUC payer with multiple options for service providers should be able to more their RUC account and services easily from one service provider to another. This right to portability is essential to an open, commercial market for providing RUC services.

Recommendation: A RUC payer should have the right to access, the right to inquire, and the right to examine personal information as well as the right to rectify errors or

inaccuracies in personal information and the right to erasure of location and metered use data after it is no longer needed following a specified period. Exceptions to erasure may include consent of the RUC payer, retention of anonymized aggregated information used for traffic management and research, and monthly summaries of metered use for accounting purposes.

3.2.3.2 Informing RUC payers of their rights

If a state establishes certain rights for RUC payers pertaining to their RUC information, the rights will only have import and proper effect if the persons affected have knowledge of them and specifically how to exercise them.

Recommendation: At the outset of the engagement, service providers for a RUC system should provide payers information of their rights pertaining to personal information and specifically how to exercise them.

3.2.3.3 Responding to a request for exercise of rights

The manner of response to the RUC payer's request for exercise of rights should not be left to the discretion of the service provider. To enable a response empowering the RUC payer's ability to exercise their rights, the specific requirements for the response should be described in law and a service provider must never refuse a request for exercise of rights.

To ensure transparency, a service provider should inform a RUC payer when the service provider decides not to comply with a request and the reasons for the noncompliance. A non-response would leave the RUC payer with no information upon which to seek remedies.

Recommendation: The specific requirements for responding to a request for exercise of rights—transparency, intelligible, easily accessible, clear and plain language—should be described in law. A service provider must never refuse a request for exercise of rights. Nevertheless, a service provider should inform a RUC payer when the service provider does not to comply with a request and the reasons for the noncompliance.

3.2.4 Consent

A privacy policy for a RUC program may include two types of consent should the policy allow for exceptions to protection of privacy for personal information. Generally, consent

means any freely given, specific, informed, unambiguous indication of the RUC payer's wishes. Another, and more specific, type of request is express approval of the entity with which personal information will be shared. It is important for RUC payers to approve precisely to whom and where their personal information goes. The OReGO program uses express approval in this manner to enable service providers to sell value-added services to RUC payers. This has the potential to reduce the cost of administration for a RUC program by allowing service providers to bundle services.

Not all consent requires the specificity of express approval. For example, approval of a service provider's retention of location and daily metered use data beyond the time limit would not require identification of an entity for sharing.

A RUC payer may change his or her mind about granting consent or express approval. In these case, a RUC payer should have the ability to withdraw consent or express approval.

Recommendation: The model privacy policy should define consent as any freely given, specific, informed, unambiguous indication of the RUC payer's wishes. The model privacy policy should provide for express approval for sharing of personal information with a specific entity. A RUC payer should be able to withdraw consent of express approval.

3.2.5 Treatment of RUC payers

Service providers may desire to treat RUC payers who exercise their rights differently than other RUC payers, either by charging fees or whether to provide services at all. For example, a service provider may refuse to provide service to a RUC payer who refuses to give express approval to sharing of personal information with a specific entity. In a fully-competitive, open, commercial market, such refusal may not prove impactful to RUC payers if they have an assortment of choices for service provision that offer an alternative. Until a fully-competitive, open, commercial RUC market develops, such refusal could be considered a discriminatory action reducing or even eliminating the rights of RUC payers. On the other hand, a service provider may be allowed to offer a different price to RUC payers for services as long as the price is directly related to the value provided.

Recommendation: A model privacy policy should prohibit service providers from engaging in discriminatory behavior against RUC payers for exercising their rights. A service provider may offer a different price to RUC payers for services as long as the price is directly related to the value provided.

3.2.6 Security

3.2.6.1 Security measures

Given the frequency and significance of data breaches in recent years, any new tax collection program that bases its calculation on sensitive information must have effective security measures. The integrity of, and public regard for, a RUC program will depend upon it. The security of RUC information held by service providers must be assured by application of appropriate technical and organizational security measures that ensure a level of security appropriate to the risk of disclosure.

Recommendation: A model privacy policy should require a service provider to implement security measures to protect personal information to a level appropriate to the risk of disclosure.

3.2.6.2 Security breach notices

Data breaches happen and they will happen, eventually, in a RUC system. To maintain positive public regard, a RUC system must assure the transparency of any data breach that occurs. This will require service providers to provide notice and details of the breach to the authorized agency as the oversight authority with responsibility to manage service provider performance. Service providers should provide notice of the breach to RUC payers if the service provider has not implemented appropriate security measures or managed the breach appropriately.

Recommendation: A model privacy policy should require a service provider to provide notice to the authorized agency when a breach happens and provide specific information to the authorized agency about the nature of the breach and its likely impact. Service providers should provide notice to RUC payers of any breach where the service provider has not implemented appropriate security measures, has not taken subsequent measures to reduce high risk or has not made an effective public communication about the breach.

3.2.7 Compliance

The GDPR in the European Union requires appointment of a data protection officer with defined tasks and responsibilities to ensure compliance with that privacy regulation. Such a person designated as contact for RUC payers exercising their rights and ensuring compliance with the requirements to protect personal information would enable similar assurance for a RUC system.

Recommendation: The model privacy policy should require a service provider to designate a personal information officer with the responsibility as contact for RUC payers and to ensure compliance.

3.2.8 Certification

Service providers for a RUC system should prove they can perform the required services before they get approval from the authorized agency to provide the services. This requires the authorized agency to establish certification mechanisms for service providers to demonstrate compliance with the model privacy policy.

An authorized agency may develop and apply the certification process for service providers to achieve accreditation. ORe*GO* uses such a certification process for its service providers. Alternatively, the authorized agency may rely upon certification bodies to provide the process for service providers. Rather than develop individual certification processes from scratch and at significant cost to maintain this capability, it would behoove states to rely upon independent certification bodies to certify the service providers according to criteria set by the authorizing agency, especially if the states work together to select the appropriate certification bodies to apply common criteria. Certification bodies should be accredited by a competent supervisory authority or a national accreditation body.

Recommendation: The model privacy policy should require an authorized agency to establish certification mechanisms for service providers to demonstrate compliance with the privacy protection provisions. Certification bodies should issue and renew certifications on the basis of criteria set by the authorizing agency.

3.2.9 Remedies

A privacy protection program will only be as effective as the remedies available to enforce violations. General privacy protection laws in California and the European Union apply the following remedies, among others.

- The right to lodge a complaint with the authorizing agency;
- The right to an effective judicial remedy against a decision of an authorizing agency;
- The right to an effective judicial remedy against a service provider;
- The right to compensation for damages on account of behavior of service providers;
- Civil penalties for service providers who fail to cure violations of this policy;
- Specific civil penalties paid to aggrieved persons for security provision violations by service providers;
- The right for a public interest organization to present a claim or rights of an aggrieved person.

Recommendation: Washington should adopt an appropriate assortment of remedies to enable aggrieved RUC payers to seek redress for violation of their rights. The legislature should determine the precise nature of the set of remedies and the penalty amounts.

3.2.10 Choice of reporting methods

Oregon's RUC program offers motorists the choice of reporting method from at least two mileage reporting methods at least one of which does not require use of locational information, including specific origins or destinations, travel patterns or times of travel. This allows the RUC payer to assure that his or her preferences to use or not use location-aware reporting devices will be honored by personal preference.

This method of privacy-by-design may not be appropriate for states not allowing choices of mileage reporting options. Whether providing choice of reporting method can prove effective privacy-by-design will be determined by the type of reporting adopted in each state. This provision should therefore form part of the substantive portion of the authorizing legislation rather than as part of the model privacy protection provisions.

Recommendation: The model privacy policy need not include requirements for motorist choice of reporting method; rather such a provision should form part of the substantive portion of the authorizing legislation for a road usage charge program.

3.2.11 Preemption

State laws often preempt local governments from enacting law that conflicts with the state's laws. In most states, the state's constitution automatically preempts local laws that conflicts with state laws unless an exception is enacted.

Recommendation: In most states, a preemption clause is unnecessary and therefore not included in the model privacy policy.

3.2.12 Anonymization of information and data

The Model California Road Charge Privacy Legislation suggests an anonymization requirement for RUC information and data held by a service provider. This may add cost for no real benefit since the broader model privacy policy requires erasure of the location and metered use data within 30 days after this information is no longer needed for payment, dispute resolution or noncompliance investigation. When RUC payer has consented to a retention of location and metered use data for longer than the 30-day period, the data should be anonymized to protect a possibly indefinite retention period.

Recommendation: The model privacy policy should require anonymization of location and daily metered use data if a RUC payer consents to retention of the data beyond the 30-day erasure period following the later of payment, dispute resolution or noncompliance investigation.

3.2.13 Record of access

The Model California Road Charge Privacy Legislation suggests a requirement for a service provider to maintain a record of access to personal information in its possession. This requirement provides transparency for any audit, investigation pertaining to a data breach or exercise of the right of examination.

Recommendation: The model privacy policy should require a service provider to maintain a record of access to personal information the service provider holds.

3.3 European Union GDPR additional topics

The European Union's General Data Protection Regulation protects general consumer data on the Internet rather than specific data like data required for a RUC program. Some of the privacy protections provisions of the EU GDPR will not be appropriate or necessary for a RUC program. An assortment of these provisions are as follows.

- Right to restriction of, or object to, processing of personal data. Under the EU GDPR, this right applies to persons whose personal data ends up in a processor's possession without having given express consent. The location and/or daily metered use data provided for a road usage charge program is fundamental to participation in the program. If participants in a road usage charge program were to have the right to restrict or stop processing of this data, it is essentially the same as withdrawing from the program. The right to withdraw from the program is already available for a volunteer road usage charge program. There would be no right to withdraw from a mandatory road usage charge program. Therefore, the right to restrict processing or the right to object to processing personal travel data is unnecessary for a voluntary program and inappropriate for a mandatory program.
- Right to decision-making not based solely on automated processing. How to look at this issue depends on the type of road usage charge program enacted by a state's legislature. If a road usage charge program requires electronic reporting of vehicle travel data to calculate the charge, automatic processing is a fait accompli. If a road usage charge program offers motorists a choice between electronic reporting and manual reporting of vehicle travel data, then offering an alternative to automated processing makes this provision unnecessary.
- Broad requirements for controllers and processors of personal data. Service providers for a road usage charge program have specific functions approved by the authorized agency that are replete with performance standards and contractual requirements. Imposing broad regulatory requirements to these already-regulated functions is unnecessary.
- Requirements for a data protection and impact assessment and prior consultation. It will be necessary for road usage charge programs that use nongovernmental service providers to certify them as meeting criteria approved by the authorizing agency. During this certification process,

service providers who become certified will have successfully undertaken a data protection and impact assessment appropriate for providing road usage charge services. Undergoing an additional general data protection and impact assessment is unnecessary.

- Codes of conduct and monitoring of compliance thereto. The EU's GDPR requires establishment of codes of conduct and monitoring of compliance related to general data protection. A certification process for a road usage charge program should have performance standards that include codes of conduct directly related to services pertaining to collection of vehicle travel data. Additionally, the authorized agency's contracts with service providers should contain oversight provisions specifically related to road usage charge services. Imposing codes of conduct for general data protection and associated monitoring of compliance is unnecessary.
- Independent supervisory authorities. The EU's GDPR requires each member state to establish at least one independent supervisory authorities to monitor application of the regulations. The model privacy policy assumes that state legislatures will bestow similar authority on the authorized agency in a road usage charge program.

3.4 California Consumer Privacy Law additional topics

The California Consumer Privacy Law protects general consumer data on the Internet rather than specific data like data required for a road usage charge program. Some of the privacy protections provisions of the California Consumer Privacy Law will not be appropriate or necessary for a RUC program. An assortment of these provisions are as follows.

- Statutory restriction on sale of personal data. The model privacy policy for road usage charge programs places the RUC payer in the position of making the decision whether to expressly approve any sharing of personal information with another entity whether or not a sale of personal information is involved. If the RUC payer decides not to expressly approve of a service provider sharing personal information with another entity, then the sharing will be barred. Giving the RUC payer the decision-making authority over any sharing of personal information is much stronger than merely restricting sale.

- Right to opt out and opt in. Road usage charge programs that are voluntary in nature, like ORe*GO*, already have opt-in, opt-out built into them. For mandatory road usage charge programs, the ability to opt-in or pot-out would be inappropriate.
- Civil action brought by Attorney General. Some states may decide to involve the state's attorney general in the enforcement regime of a road usage charge program. Whether to make the attorney general central to enforcement for a road usage charge program is up to the individual state.

4 EXISTING PRIVACY LAWS FOR MOTORIST INFORMATION IN WASHINGTON

4.1 Department of Licensing collection of personal information

The state of Washington's Department of Licensing (DOL) collects and protects discovery of sensitive personal information contained in the vehicle registry and driver identity records required by state law. The DOL uses information from the vehicle registry to apply laws requiring vehicle licensing, registration and titling. The DOL uses driver licensing and identification records to apply laws requiring licensing of drivers and permit holders and providing an identification card opportunity for non-drivers.

To perform these functions, DOL maintains records identifying residents of the state, identifying their vehicles and some of their characteristics and behaviors that are of a personal nature. Existing federal and state laws require DOL to implement protective measures against disclosure and inappropriate use of this sensitive information.

4.2 Privately-operated vehicle licensing offices

The DOL appoints several privately-operated vehicle licensing offices for each county as subagents to perform vehicle licensing-related services for drivers in Washington. A subagent is a private business which enters into a contract with a county auditor to perform vehicle title and licensing services. The DOL may approve an entity as a subagent for this purpose following a request by a county for an additional subagent provided the county conducts an open, competitive process for the opportunity.

Subagents perform the following vehicle-related functions on behalf of DOL,

- Renewal of vehicle tabs
- Obtaining new license plates
- Reporting vehicle sales or transfers of ownership
- Registering vehicles

- Purchasing trip permits
- Obtaining replacement titles
- Obtaining disabled parking placards or tabs

Necessarily, private sector entities operating as subagents collect sensitive personal information while servicing vehicle owners on behalf of the Department of Licensing.

4.3 Data retained by vehicle licensing offices for Washington RUC pilot

In the Washington Road Usage Charge Pilot Project, Washington's vehicle licensing offices (VLOs) tested various methods to gather mileage data used to calculate a per-mile road usage charge for participating motorists. Specifically, these offices collected personal information such as participant identity, vehicle information and total mileage driven during a reporting period.

For the pilot, the state's VLOs collected mileage data through a manual reporting method that does not involve wireless reporting nor collection of vehicle location data. To report mileage driven, participating motorists visited one of several designated VLOs for this purpose. These motorists accessed a smartphone provided by the VLO, took pictures of their vehicle's odometer and license plate and submitted the two photographs to the project team using a web application. The VLOs retained a log that the submission occurred, the date of submission and the driver's name and vehicle identification. The VLOs did not have access to or ability to retain submitted mileage data.

4.4 Privacy laws for management and protection of driver and vehicle-related personal information in Washington

4.4.1 The Driver's Privacy Protection Act of 1994

The Department of Licensing complies with the federal Driver's Privacy Protection Act of 1994 which prohibits the disclosure of personal information of motorists without their express consent. This obligation also applies to authorized recipients of personal information such as subagents for vehicle licensing services.

Under the law, the DOL and subagents may use personal information to perform their duties pertaining to driver and vehicles licensing. There are exceptions for use of personal information for production of statistical reports and research, bulk distribution of surveys and in court and by insurance companies, licensed private investigations and private toll facilities, among a few other transportation and business-related exceptions. This law allows individual states to allow other uses of this personal information.

Not simply applicable to distributors of personal information, this law also applies to receivers of driver's personal information for unlawful purposes. This law proscribes these receivers from making false statements to obtain personal information.

Criminal fines apply for noncompliance with this law. Drivers have a civil cause of action against those who unlawfully obtain their personal information.

Under the federal Driver's Privacy Protection Act, "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address, telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status. Thus, the information protected by the federal Driver's Privacy Protection Act applies only to a portion of the information gathered by the Department of Licensing. Further protection of sensitive information comes under Washington state law, as discussed in subsection 4.4.2.

4.4.2 Washington statutory law for protection of driver information

The Revised Code of Washington (RCW 46.12.630) protects from unauthorized disclosure lists of registered and legal owners of motor vehicles held by the Department of Licensing and other authorized entities and persons. This statute directs the DOL to provide owners lists to the manufacturer of the vehicles and permits DOL to provide lists only to the following other entities for the purposes specified,

- Manufacturers of motor vehicles, legitimate businesses, or their authorized agents to conduct research activities and production of statistical reports provided the information is not used for publishing, re-disclosure or contacting individuals;

- Any governmental agency of the United States or Canada, including political subdivisions, or its authorized agents, for enforcement of traffic laws;
- Insurers for purposes of claims investigation activities, antifraud activities, rating or underwriting;
- Any local government agency, or its agents for notification relating to towed or impounded vehicles;
- A government agency, commercial parking company, or its agents for notifications relating to outstanding parting violations;
- An authorized agent or contractor of the DOL for providing motor vehicle excise tax, licensing, title, and registration information to motor vehicle dealers;
- Any business regularly making loans to finance purchases of motor vehicles;
- A company or its agents operating a toll facility to identify toll violators.

Before DOL may release any lists of motor vehicle owners to any of these entities, DOL must enter into a contract with the entity. The contract must include requirements for the conduct of regular permissible use and data security audits demonstrating compliance with data security standards adopted by the Office of the Chief Information Officer.

This statute prohibits all the approved entities from releasing personal information for direct marketing purposes. The statute defines “personal information” in the same terms as the federal Driver’s Privacy Protection Act of 1994. The statute specifically proscribes release of an individual’s photograph, social security number or any medical or disability-related information for any purpose, describing this information as *highly restricted personal information.*

The penalty for using a list of registered and legal owners of motor vehicles for nonauthorized purposes is denial of further access to the information. The Washington Administrative Code (WAC 308-10-075(8)) requires assurance from receivers of information from DOL that the information is not used for a purpose contrary to the access agreement entered into with DOL. If this assurance is violated, the rule indicates the violator will be charged under the perjury laws of the state of Washington.

4.5 Comparison of information collected for RUC and DOL systems

The information collected by a road usage charge system and DOL is similar but *not* identical. The table below compares the information collected for both systems.

Table 4-1		
Comparison of Personal Information Collected in RUC and DOL Systems	**RUC System**	**DOL System**
Name	Yes	Yes
Access information	Yes	Yes
Driver ID number	Yes	Yes
Vehicle ID number	Yes	Yes
Vehicle plate number	Yes	Yes
Vehicle registration	Yes	Yes
Financial information	Yes	Potentially
Payment record	Yes	Yes
Date of Birth	No	Yes
Sex	No	Yes
Marital status	No	Yes
Organ donor status	No	Yes
Social security number	No	Yes
Permit number	No	Yes
ID card number	No	Yes
Vehicle title	No	Yes
Photograph	No	Yes
Proof of identity	No	Yes
Driving record	No	Yes
Vision exam report	No	Yes
Medical exam report	No	Yes
Hazardous materials endorsement	No	Yes
Penalties imposed	No	Yes
Alcohol or drug violations	No	Yes
Driving test results	No	Yes
Liability insurance	No	Yes
Veteran designation	No	Yes
Disabled parking eligibility	No	Yes
Vehicle report of sale	No	Yes
License suspensions	No	Yes
RUC Account ID number	Yes	No
ID code for mileage meter	Yes	No
Distance traveled data	Yes	No
Travel data record	Yes	No
RUC enforcement record	Yes	No

5 MODEL RUC PRIVACY POLICY FOR STATES

The model privacy policy was developed to guide legislative activity for Washington (and prospectively other states) on the issue of privacy protection in the context of a RUC program. This model privacy policy examined recent privacy policy law enactments in Oregon and the European Union and the state of California to compile a comprehensive policy proposal.

GENERAL PROVISIONS	
Stated Purpose	This policy protects personal information collected pursuant to a Road Usage Charge Program from disclosure. A ***Road Usage Charge Program*** is a statutory program, supported by administrative rules, for collecting road usage charges for metered use of a subject vehicle on the highways of the state.
Protected information	***Personal information*** means information or data that identifies, relates to or describes a person or entity that is obtained or developed in the course of reporting metered use by a subject vehicle, including but not limited to travel pattern data, or for providing administrative services related to the collection of road usage charges. ***Personal information*** does not include anonymized information or anonymized aggregated information. ***Anonymized information*** means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person, provided a service provider has implemented technical safeguards and processes that prohibit re-identification of the person, processes that prevent inadvertent release of the information and makes no attempt to re-identify the information. ***Anonymized aggregated information*** means aggregated information accumulated in a way that preserves the anonymity of the persons reporting metered use by a subject vehicle related to collection of a road usage charge and cannot create travel pattern data nor reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person. ***Travel pattern data*** means location and daily metered use data of a subject vehicle and data that describes a person's travel habits in sufficient detail that the person becomes identifiable either through the data itself or by combining publicly available information, or information available to the service provider, with the data.
Material Scope	This policy applies to processing of personal information reported by a road usage charge payer for a subject vehicle wholly or partly by automated or other means for purposes of paying a road usage charge for metered use by a subject vehicle of the highways of the state. ***Processing*** means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means. A ***road usage charge payer*** means a registered owner or lessee of a subject vehicle.

	Registered owner means a person, other than a vehicle dealer, that is required to register a motor vehicle in the state. ***Lessee*** means a person that leases a motor vehicle that is required to be registered in the state. ***Subject vehicle*** means a motor vehicle that is subject to the Road Usage Charge Program.
Territorial Scope	This policy applies to the processing of personal information by a commercial or government entity, whether established in the state or not, where activities relate to collection of a road usage charge irrespective of payment.

PRINCIPLES

Principles for lawful processing of personal information

An authorized agency shall ensure protection of the confidentiality of personal information used for reporting metered use by a subject vehicle or for administrative services related to the collection of the road usage charge under its authority.

[If a state's public records laws grant public access to driving records,] personal information used for reporting metered use by a subject vehicle or for administrative services related to the collection of the road usage charge is a public record exempt from disclosure.

Information collected for use in a Road Usage Charge Program shall be accurate, relevant and collected and processed in a transparent manner only for use in collecting a road usage charge from a road usage charge payer for a subject vehicle. The personal information shall be kept in a form which permits identification of the subject vehicle and its registered owner or lessee no longer than necessary and processed in a manner that ensures appropriate security, using appropriate technical or organizational measures.

No person or entity involved with collection of a road usage charge may disclose personal information used or developed for reporting metered use by a subject vehicle or for administrative services related to collection of road usage charges to any person, except to the following recipients limited to the information necessary to the respective recipient's function in collecting road usage charges:

- the road usage charge payer;
- a financial institution, for the purpose of collecting road usage chargers owed;
- employees of the authorized agency;
- a service provider;
- a contractor for a service provider, but only to the extent the contractor provides services directly related to an agreement with the authorized agency;
- an entity expressly approved to receive the information by the road usage charge payer for the subject vehicle;
- a police officer pursuant to a valid court order based on probable cause and issued at the request of a federal, state or local law enforcement agency in an authorized criminal investigation involving the person to who the requested information pertains.

An authorized agency or service provider that accesses or provides access to personal information shall maintain a record of that access. The access control log shall include:

- Date and time the information is accessed;
- The data elements used to query the road usage charge database or system;
- The person accessing the personal information;
- The purpose for accessing the information.

	A ***service provider*** means an entity that has entered into an agreement with the authorized agency for reporting metered use by a subject vehicle or for administrative services related to the collection of road usage charges, and authorized employees and contracted entities of the entity. The state may appoint a state agency to act as a service provider as an alternative to a contracted service provider. ***Authorized agency*** means a government agency assigned the responsibility and given the authority by authorizing legislation to implement and operate the Road Usage Charge Program. ***Express approval*** means active approval, either electronic or on paper, by a road usage charge payer that identifies the entity with which personal information will be shared. The request for express approval must be clearly distinguishable, intelligible and easily accessible in clear and plain language. If this provision is infringed, the express approval will not be binding. The person providing personal information has right to withdraw express approval at any time. Withdrawal of express approval shall not affect lawfulness of express approval given before withdrawal provided the person was informed thereof. It shall be as easy to withdraw as give express approval.
RIGHTS	
Right to transparency and modalities	The service provider shall provide information related to rights pertaining to personal information in writing, or where appropriate, by electronic means, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information may be provided orally if requested by the road usage charge payer. The service provider shall post the information on its website and also deliver the information within 10 days of receipt of a request for this information from a road usage charge payer or a representative of the road usage charge payer. The service provider shall facilitate the exercise of these rights and shall not refuse to act upon the request of a road usage charge payer. The service provider shall provide information upon a request for exercise of rights pertaining to personal information without undue delay and no longer than 15 days of receipt of a request. Where request is made by electronic means, the information can be provided by electronic means. The time period for compliance may only be extended for a reasonable time period in order to confirm the identity of the road usage charge payer or the legal status of the road usage charge payer's representative. If service provider does not take action on the request of the road usage charge payer, the service provider shall inform the road usage charge payer, without delay, but no later than one month after receipt of the request of the reasons for not taking action and the possibility for lodging a complaint with the authorizing agency and seeking judicial remedy.

Rights to provision of information where personal information is collected from a road usage charge payer	At the time when the service provider obtains personal information from the road usage charge payer, the service provider shall provide the road usage charge payer the following information free of charge in an easily visible, intelligible and clearly legible manner, to ensure fair and transparent processing: • identity and contact details of the service provider; • contact details of the designated personal information officer which the service provider has assigned responsibility for managing personal information protection and rights thereto; • the period of storage or criteria to determine that period; • existence of the right to request access to and rectification or erasure of personal information and the right to portability; • recipients, or categories of recipients, of the personal information, if any. • the existence of right to withdraw consent at any time without affecting the lawfulness of the processing on the prior consent or express approval; • the right to lodge a complaint with the authorized agency; • whether the provision of personal information is a statutory or contractual requirement, or necessary to enter into a contract, and whether the road usage charge payer is obliged to provide personal information and possible consequences of failure to do so.
Right to access by road usage charge payer	A road usage charge payer has the right to inquire about the nature, accuracy, status and use of personal information and the right to examine the personal information, or a reasonable facsimile thereof. A road usage charge payer has the right to lodge a third-party complaint with the authorized agency. The service provider shall respond to requests for inquiry or examination within five business days of receipt of the request. The service provider shall disclose and deliver the requested personal information free of charge. The information may be provided by mail or electronically and if so portably and in a readily useable format that allows the road usage charge payer to transmit this information to another service provider or the authorizing authority without hindrance.
Right to rectification	The road usage charge payer has the right to request rectification of personal information upon provision of reasonable evidence that the information has errors or has changed. The service provider shall respond to requests rectification within five business days of receipt of the request.

Right to erasure	Not later than 30 days after completion of payment processing, dispute resolution for a single reporting period or a noncompliance investigation, whichever is latest, the service provider shall erase records of the location and daily metered use of subject vehicles. The road usage charge payer has the right to erasure of personal information no longer necessary to fulfill duties under the Road Usage Charge Program without undue delay and the service provider has the obligation to erase personal information no longer necessary to fulfill duties under the Road Usage Charge Program without undue delay. ***Non-compliance investigation*** means an investigation by the authorized agency to determine if, and to what extent, any person, including but not limited to a road usage charge payer, is in compliance with the statutory provisions of the Road Usage Charge Program and associated administrative rules. Such investigations may include informal inquiries or a formal review of the relevant records and the mileage reporting method of the road usage charge payer or manager of accounts to ascertain the extent of non-compliance, if any. The road usage charge payer for a subject vehicle has the right to erasure of the location and daily metered use data that has not been destroyed within the required period of time. The service provider shall respond to requests for erasure within five business days of receipt of the request. Exceptions: • Records accumulated as anonymized aggregated information may be retained and used for purposes of traffic management and research. • Monthly summaries of metered use by subject vehicles retained by the authorized agency or a service provider that include vehicle identification numbers of subject vehicles and associated total metered use during the month but not location information. • A service provider may retain and use records of location and daily metered use of subject vehicles if the road usage charge payer for the subject vehicle consents to the retention. In this context, consent means voluntary agreement given to retain location and daily metered use data beyond the period required by law. Consent does not entitle the authorized agency to obtain or use the records or the information in the records. Any records retained by authority of consent of the road usage charge payer shall be anonymized. The right of erasure shall not apply to the extent processing is necessary for compliance with a legal obligation or establishment, exercise or defense of legal claims. The service provider shall communicate any rectification or erasure of personal information to each recipient to which personal information were disclosed and inform road usage charge payers about recipients, if requested.
Conditions for consent	***Consent*** means any freely given, specific, informed and unambiguous indication of the road usage charge payer's wishes signifies agreement to collection and processing of metered use data for use in assessing a road usage charge. A road usage charge payer has the right to withdraw consent at any time. Withdrawal of consent shall not affect lawfulness of consent given before withdrawal provided road usage charge payer was informed thereof. It shall be as easy to withdraw as give consent.
Right to portability	A road usage charge payer has right to receive personal information provided to a service provider in a secure, structured, commonly used and machine-readable format and has the right to transmit that personal information to another service provider without hindrance. A road usage charge payer has the right to have personal information securely transmitted directly from one service provider to another where technically feasible.

No discrimination for exercise of rights	A service provider shall not discriminate against a road usage charge payer because the road usage charge payer did not give express approval to the service provider to enable sharing of personal information. A service provider may offer a different price, rate, level, or quality of goods or services to the road usage charge payer if that price or difference is directly related to the value provided to the road usage charge payer by the road usage charge payer's personal information. A service provider shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.
SECURITY	
Security of processing	The service provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of destruction, loss, alteration, unauthorized disclosure of or access to personal information, including but not limited to the following: • pseudonymization and encryption of personal information; • ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services; • ability to restore availability and access to personal information in a timely manner in event of an incident. ***Pseudonymization*** means the processing of personal information in a manner that renders the personal information no longer attributable to a specific road usage charge payer without the use of additional information.
Notification of personal information breach	For a personal information breach, the service provider shall without undue delay and where feasible, not later than 72 hours after awareness of it, notify the breach to the authorized agency unless it is unlikely there is risk to rights and freedoms of natural persons. Where notice is not made within 72 hours, it shall contain reasons for the delay. The notification shall: • describe the nature of the personal information breach, including the categories and approximate number of road usage charge payers and personal information records involved; • communicate the name and contact details of the designated personal information officer of the service provider or other contact; • describe the likely consequences; • describe the measures taken to address the personal information breach, its effects and remedial action taken, including measures to mitigate. This information may be provided in phases where this information cannot be provided at the same time.
Communication of personal information breach to road usage charge payers	Where a personal information breach is likely to result in high risk to rights and freedoms of natural persons, the service provider shall communicate the breach in clear and plain language to the road usage charge payer without delay. The communication shall not be required if: • service provider has implemented appropriate technical and organizational measures which were applied to the personal information affected by the breach; • service provider has taken subsequent measures which ensure high risk to rights and freedoms of road usage charge payers are unlikely to materialize; • it would involve a disproportionate effort and a public communication is made that is equally effective.

	If the service provider makes no communication about a personal information breach, the authorized agency may require a service provider to do so.
PERSONAL INFORMATION OFFICER	
Designation of personal information officer	A service provider shall designate a personal information officer to enable contact with road usage charge payers and the authorizing agency for purposes of assuring compliance with this policy. The designated personal information officer may be a staff member of the service provider (or fulfill the tasks on the basis of a service contract) but shall be designated on the basis of professional qualities and expert knowledge of personal information protection under this policy and practices and ability to fulfill tasks.
Organizational usage and privacy policy	The authorized agency and service providers shall establish, publish and adhere to an organizational usage and privacy policy. The organizational usage and privacy policy shall be available in writing to road usage charge payers, and shall be posted conspicuously on the authorized agency's website and each service provider's website. The organizational usage and privacy policy shall include: • The authorize purpose for collecting personal information; • The identity and designated tasks for the personal information officer; • Description of the employees and contractors authorized to access and collect personal information and identification of training requirements necessary for the employees and contractors; • Description of how the personal information shall be monitored to ensure compliance with applicable privacy laws and a process for periodic system audits; • Description of reasonable measures that will be used to ensure the accuracy of the personal information and correction of information errors; • Description of how compliance with security procedures and practices will be implemented and maintained; • Description of how compliance with the rights of road usage charge payers designated by this policy will be maintained; • The period for which the personal information will be stored or retained, by category; • The purpose of, and process for, sharing or disseminating personal information with other persons, whether by those authorized under this policy or by consent of motorists under this policy.
CERTIFICATION	
Certification	The authorized agency shall establish certification mechanisms for service providers to demonstrate compliance with the requirements of this policy. Certification bodies shall issue and renew certification on the basis of criteria approved by the authorizing agency. Certification may be withdrawn where requirements for certification are no longer met.
Certification bodies	Independent certification bodies shall be accredited by a competent supervisory authority or a national accreditation body. Certification bodies shall be accredited for a maximum of five years according to certain criteria established by a competent supervisory authority or a national accreditation body.

REMEDIES	
Right to lodge complaint with authorized agency	Every road usage charge payer has the right to lodge a complaint with an authorized agency which shall inform the complainant on the progress and outcome of the complaint and the possibility of judicial remedy.
Right to effective judicial remedy against authorized agency	Each road usage charge payer has rights to an effective judicial remedy against a legally binding decision of an authorized agency concerning them. Each road usage charge payer has a right to an effective judicial remedy where the authorized agency does not handle a complaint or does not inform the road usage charge payer within 3 months on the progress or outcome of complaint lodged.
Right to effective judicial remedy against service provider	Without prejudice against any other available administrative or non-judicial remedy, each road usage charge payer has the right to an effective judicial remedy where rights are considered to have been infringed by a service provider in non-compliance with this policy.
Representation of road usage charge payers	A road usage charge payer has the right to mandate that a properly constituted public interest organization present a claim or rights on his/her behalf.
Rights to compensation and liability	Road usage charge payers shall have the right to compensation for damages suffered by the actions of service providers which infringe upon rights and responsibilities contained in this policy.
General conditions for imposing administrative fines / Civil actions	Any service provider shall be in violation of this policy for failing to cure any alleged violation within 30 days after notification of alleged noncompliance and therefore liable for civil penalty. Any service provider that intentionally violates this policy shall be liable for a civil penalty of up to $XXXX for each violation but may be adjusted as necessary to ensure the costs incurred by the state are covered.
Civil action for security violations	Any road usage charge payer whose personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty of to implement and maintain reasonable security practices may institute a civil action to recover damages not less than $XXX or greater than $XXX per incident or actual damages, based on circumstances, whichever is greater, injunctive or declaratory relief, or any other relief the court deems proper.
MISCELLANEOUS	
Compliance with other laws	This policy does not affect compliance with other federal, state or local laws or civil, criminal, or regulatory inquiries, investigation, or subpoenas or summons issues by federal, state or local authorities or cooperation with law enforcement agencies.
Regulations	The authorized agency shall solicit broad public participation to adopt regulations on or before the operative date for this policy.
Attempts to avoid the reach of this policy	If a series of steps or transactions were component parts of a single transaction intended to avoid the reach of this policy, a court shall regard the intermediate steps or transactions.
Inapplicability of waiver	Any provision in a contract that purports to waive or limit road usage charge rights under this policy shall be void and unenforceable.

6 APPLICATION OF THE MODEL PRIVACY POLICY FOR A ROAD USAGE CHARGE SYSTEM IN WASHINGTON

6.1 Existing privacy law applications in Washington in context of the Model RUC Privacy Policy

Washington state applies existing state and federal law to protect sensitive personal information obtained by the Department of Licensing in the performance of its statutory duties. A road usage charge system must access similar personal information to enable collection of road usage charges. The purpose of each program differs enough, however, to indicate that a separate privacy law should be enacted simply for the protection of personal information in a RUC system albeit one aligned with the existing statutory protections for information contained in the state's vehicle registry. This section compares the existing driver privacy protections in Washington with those of the Model RUC Privacy Policy and draws a conclusion about how personal information in a RUC system could be afforded the best protection.

6.2 Protected information

As table 4-1 indicates, much of the information DOL collects to perform the agency's mandated activities is not required for collection in a road usage charge system. Information related to the ability to drive, driving record, violations, record of insurance and various statuses are simply not relevant to collection of a road usage charge. Similarly, some of the information collected by a road usage charge system is not relevant for collection by DOL, such as distance traveled data, travel data record, RUC account identification number, identification code for a mileage meter and RUC enforcement record. Therefore, to protect personal information collected in a RUC system, an application of the Model RUC Privacy Policy would require a definition of *personal information* aligned completely with RUC.

6.3 Territorial scope

The application of the Model RUC Privacy Policy to commercial or private entities will depend upon the particular RUC system adopted in the state of Washington. The Washington RUC pilot used private sector entities to collect travel data and RUC revenue

and manage a RUC account for each payer. Alternatively, a RUC system could have a government agency perform these activities. Or, there could be options for both private and public entities administering RUC accounts. Whichever RUC system is ultimately adopted, the entities performing RUC administrative activities must comply with the privacy protection provisions in a RUC law.

6.4 Principles for processing of personal information

In a road usage charge program adopted in Washington state, it will be necessary for the entities involved with collection of RUC data and revenue to be able to access the state's vehicle registry. Therefore, any RUC legislation passed must allow these entities to obtain lists of the vehicle registry and the associated registered owners or lessees and require these entities to enter into a contract with DOL in accordance with RCW 46.12.630. To align with this existing statute, this contract must include requirements for the conduct of regular permissible use and data security audits that demonstrate compliance with data security standards adopted by the Office of the Chief Information Officer.

Restrictions on disclosure of personal information in a RUC system would differ from those for DOL. The relevant statute mandating protection of DOL information, RCW 46.12.630, is less specific about who can use protected information, leaving the specifics to the contractual discretion of DOL, while the Model RUC Privacy Policy specifically names other recipients which can use personal information in the performance of their respective functions in collecting road usage charges. Nevertheless, the two policies should integrate well with DOL regulating access to the personal information it holds and manages.

6.5 Rights

The laws governing DOL do not establish statutory rights for access, rectification, erasure, portability and conditions for consent as does the Model RUC Privacy Policy. Should issues pertaining to these rights arise in the DOL system, they would be managed by establishing internal policies. Since protection of privacy is one of the leading issues for adoption of a RUC system, any legislation adopting a RUC program will likely require establishment of statutory protection of these rights.

6.6 Security

The writers of RCW 46.12.630 were certainly considering security when its provisions were drafted but they chose to allow DOL the authority to determine on a case-by-case contractual basis the nature of the security measures imposed on subject entities receiving personal information from DOL. The Model RUC Privacy Policy establishes a standard for protection of personal information collected in a RUC system and also mandates notifications of breaches. The RUC security provisions will likely be required by privacy advocates for a RUC system.

6.7 Personal information officer

The Model RUC Privacy Policy requires an entity collecting RUC data and revenues to appoint a personal information officer with specific duties relating to the payers and assurance of establishment and adherence to an internal organizational usage and privacy policy. While DOL could exercise this type of provision in a contract with recipient entities, the agency is not required to do so.

6.8 Certification

The Model RUC Privacy Policy requires certification of entities collecting RUC data and revenues to demonstrate compliance with its requirements. DOL has no certification process but could establish by contract one on a case-by-case basis.

6.9 Remedies

The only remedy RCW 46.12.630 establishes for violation of a DOL nondisclosure contractual requirement is denial of access to the lists of personal information. The Model RUC Privacy Policy's remedies are much more robust, including judicial remedies, rights to compensation, liability and administrative fines.

The federal Driver's Privacy Protection Act of 1994 is also robust as it applies to disclosure of protected information, including application of criminal fines for noncompliance with this law. Furthermore, drivers have a civil cause of action against those who unlawfully obtain their personal information.

6.10 Conclusion

While the law governing DOL's protection of personal information applies to some of the information necessary for collection of a road usage charge, it is not as robust or as

protective as the Model RUC Privacy Policy nor do the laws applicable to DOL apply to all types of personal information collected in a RUC system. Thus, protection of personal information in RUC system should occur by statutory enactment of the Model RUC Privacy Policy. Even so, because of the need for RUC collection entities to access the DOL's vehicle registry, the two public policies should be integrated to achieve that accessibility.

7 CONCLUSION

While ensuring technical protections for personal information in a road usage charge system is important to establishing integrity for road usage charge programs, agreement on specific law-based protections will be necessary to obtain enough public confidence to enable road usage charge statutory enactments. A stringent model privacy policy energized with contemporary legal protections for consumer data in Oregon, California and the European Union should help to reduce public angst over road usage charges. Further negotiation of these privacy policies with privacy advocates in a legislative process may well calm public concerns over privacy in a road usage charge system sufficient to enable enactment of the program in law.

APPENDIX A: PRIVACY EMERGING AS A CRITICAL ISSUE

I. Privacy in early RUC investigations

The theory of charging vehicle owner/operators by the amount of distance traveled emerged during the final decades of the 20th century. Practical proposals failed to develop, however, until global positioning system (GPS) technology reached commercial viability toward the end of the century. With GPS technology installed in a vehicle, travel coordinates can reveal the location, time, and amount of vehicle travel over a specific time period for purposes of imposing a charge on distance traveled within a jurisdiction.

In the early years of distance charge development, researchers and privacy advocates quickly identified privacy protection as the fundamental hurdle for enactment of RUC legislation. The potential for collectors of GPS data to know a person's precise travel history elicited a gut reaction from nearly everyone considering the concept that most people would have strong concerns about any entity possessing that information.

Minnesota

Some of the earliest research on charging by distance traveled was done during the mid-1990s for the Minnesota Department of Transportation (MnDOT) and the Metropolitan Council under the sponsorship of the U.S. Federal Highway Administration (FHWA). The privacy issue was not an official concern stated in this research, probably because the researchers proposed collecting vehicle miles traveled through an electronic odometer device read at the fuel pump or border crossings rather than through a wireless GPS device. The 1997 Minnesota report did not specifically describe how the electronic odometer would work technologically; rather, it described only the collection of an aggregation of miles traveled with an aggregate of out-of-state miles subtracted to calculate the sum due for specific period.[6] Thus, there would be no generation or reporting of either vehicle location or travel time. A demonstration of this system was never piloted.

15-state consortium

Three years later, MnDOT and the University of Iowa formed and led a 15-state pooled fund to update the exploration of an electronically oriented distance-based RUC. This

6 Minnesota Department of Transportation and Metropolitan Council, Road Pricing Study: Final Report, March 1997.

time the central technology focus was on GPS technology. In a technical report entitled *A New Approach to Assessing Road User Charges*, the privacy issue took center stage[7].

The report analyzed the privacy issue from two perspectives. First, the report examined whether the new approach to RUC constituted an invasion of motorist privacy in light of existing privacy law in torts, administrative law, and criminal law. The report concluded, "[O]ur review of legal precedent found nothing that indicates the new approach to assessing road user charges would constitute an invasion of motorists' privacy."[8]

Secondly, the report analyzed whether and how technical safeguards could be designed to protect the privacy of motorists. Examining the technology and methods available at the time (2002), the report's authors concluded:

> "The real issues are most likely to center around implementation. How detailed the data are that the on-board computer stores for uploading to the collection center will be a prime consideration. Steps the collection center may take to ensure anonymity of the traveler when analyzing and presenting the resulting trip data also will be highly important. Additionally, it will be advisable to assure the motoring public that the only uses of the data will be for assessing road user charges and (optionally) technical analyses associated with providing transportation services[9]."

The report did not consider proposing legal constraints on the use of travel data in a RUC system, save for suggesting "criminal sanctions to regulate employee conduct."[10] Rather, the report's authors viewed the protection of privacy from the technical perspective alone, presuming that sufficient technical protections—such as securely encrypted databases—would be sufficient to garner public confidence in a RUC system.

Oregon

In 2001, the Oregon Legislative Assembly formed the Road User Fee Task Force (RUFTF) to explore a new user fee for funding the road system to replace the fuel tax.

---

[7] Forkenbrock, David J. and Kuhl, Jon G, A New Approach to Assessing Road User Charges. Transportation Policy Research. Iowa City: University of Iowa Public Policy Center; 2002.
[8] Ibid, p. 89.
[9] Ibid, p. 90.
[10] Ibid, p. 89.

The Oregon legislature also directed the Oregon Department of Transportation to test the RUFTF's proposal in a pilot test.

At the first meeting of the RUFTF on November 30, 2001, the task force learned GPS technology was likely to be tested. The task force members immediately predicted the public would demand protection of personal privacy and insisted on protection of privacy under any scenario tested.

II. Privacy as a demonstrated concern of the public

When use of GPS technology to collect travel data was only theory, there was no pushback from the public or the media. Once a government agency revealed a study to explore the use of GPS technologies for collecting data for a road usage charge, the media put a bright spotlight on the concept and assumed the worst.

The RUFTF's prediction of a public outcry came to pass following the first news story in Oregon in December 2002 that GPS devices were under consideration for use in trials.[11] During the media storm that following, privacy concerns emerged with a fury, lasting 60 straight days. No matter the political leanings of the individual media outlets, the general tone was all negative. The first neutral news story appeared in Wired Magazine five months later. The use of GPS technology in pilot tests raised suspicions.

To this day, public concerns about RUC often center on privacy, including in Washington. In the public survey conducted prior to the launch of the WA RUC pilot in 2017, 20% of respondents identified protection of personal information as the most important issue to them. In the first survey of pilot participants conducted in early 2018, privacy ranked as the top issue, with 83% of respondents characterizing it as "very important" to them.

[11] *Albany Democrat-Herald*, December 30, 2002.

APPENDIX B: LEGAL BASIS FOR FEDERAL PRIVACY PROTECTION IN THE UNITED STATES

I. Government action

The United States Constitution, including the Bill of Rights, empowers the federal government and places limits on government actions. While the U. S. Constitution does not explicitly mention a right to privacy, the United States Supreme Court has ruled on various occasions that a right to privacy exists with respect to federal or state government actions.

U. S. Supreme Court cases

The U. S. Supreme Court first recognized a constitutional right to privacy in *Griswold v. Connecticut*,[12] inferred from the penumbras of other expressly stated rights to privacy such as the right of association (the 1st Amendment), the prohibition against the quartering of soldiers in any house in time of peace without consent (the 3rd Amendment), the right against unreasonable searches and seizures (the 4th Amendment), the right against self-incrimination (the 5th Amendment), and other rights retained by the people (the 9th Amendment). The Court found that taking the penumbras together the U. S. Constitution creates a *zone of privacy.*

In succeeding cases, the Supreme Court bolstered the right to privacy by deriving the right to privacy from the right to personal liberty under the Due Process Clause of the 14th Amendment.[13] According to the Supreme Court, the Constitution protects against government action depriving persons the right of privacy. However, the Court has not inferred a government obligation to protect against access or use of private or sensitive information generally.

In *Carpenter v United States*,[14] the Supreme Court denied a government agency unrestricted access to a wireless carrier's database of physical location information unless a warrant is obtained. In the earlier case of *United States v. Jones*,[15] the Supreme Court limited the use of GPS devices by police officers to track the movement of

[12] Griswold v. Connecticut, 381 U.S. 479 (1965)
[13] Eisenstadt v. Baird, 405 U.S. 438 (1972); Roe v. Wade, 410 U.S. 113 (1973); Lawrence v. Texas, 539 U.S. 558 (2003).
[14] Carpenter v. United States, 585 U.S. ___ (2018)
[15] United States v. Jones, 565 U.S. 400 (2012)

suspects. These rulings protect individuals from government agencies having unfettered access to their personal travel information without proving probable cause. A RUC program should not have constraints on the use of data from location-aware devices as long as the use of the information obtained from these devices is limited to calculation of a RUC and cannot, by law, be used for any other purpose, such as an investigation or surveillance, without proof of probable cause.

II. Private action

Law governing private action pertaining to personal data and information come from common law or the statutory enactments of Congress or state legislatures.

Common law

Under common law, each person has the right of freedom from invasion of privacy. This right is actionable as a tort when a person wrongfully intrudes upon the private affairs or information of another person in a manner that causes mental suffering in some form. Prior to any statutory protections, the only redress available under common law was filing a lawsuit in an appropriate jurisdiction seeking an award of damages.

US statutory protections for privacy of personal data and information

The United States Congress enacted the Privacy Act of 1974 to govern the collection, maintenance, use, and dissemination of personal records about individuals held by federal agencies. The Privacy Act prohibits disclosure of personal records about an individual to third parties without the consent of the individual. There are 12 statutory exceptions. Under the Privacy Act, individuals may access their records and have them amended.

Congress has not enacted a general privacy law to protect from disclosure personal data and information held by private persons or entities. All congressional enactments protecting personal data and information held by private persons or entities are specific to certain categories of information. The following are an assortment of federal privacy protection laws for specific information in the United States:

- Children's Privacy
  - Children's Online Privacy Protection Act (online personal information of children)
- Communications

- The Electronic Communications Privacy Act, 1986 (communications interception)
- Telephone Consumer Protection Act of 1991 (telephone solicitations)

- Financial
  - Fair Credit Reporting Act, 1970 (credit records)
  - Right to Financial Privacy Act, 1978 (financial records)
  - Taxpayer Browsing Protection Act, 1997 (tax returns)
  - Gramm Leach Bliley Act (1999) (financial records)
  - Fair and Accurate Credit Transactions Act, 2003 (identity theft prevention)
- Medical
  - Health Insurance Portability and Accountability Act of 1996 (medical records)

APPENDIX C: DEVELOPMENT OF PRIVACY PROTECTION POLICIES FOR U.S. ROAD USAGE CHARGE PROGRAMS

I. Policy task forces and pilot programs of the states

Beginning with Oregon in 2001 followed by Washington in 2012 and California in 2014, state legislatures directed state agencies to work with independently-appointed bodies to adopt policies for a distance-based charge followed by demonstration in a pilot program. Protection of privacy was among the top issues for analysis and development of solutions in each state.

Oregon

Road User Fee Task Force (RUFTF). In a March 2003 report laying out recommendations for a distance charge pilot program, Oregon's Road User Fee Task Force recognized that much of the public was "uncomfortable with a government or other entity having the ability to follow vehicle movement either in real time or from travel history." The task force adopted a policy of assurance for those paying a distance-based charge that technology would not be used to violate their expectations of privacy.

The RUFTF focused on a two-track solution. One track focused solely on technology-based solutions, with focus on data transmission limitations so there would be only transfers of summary data from the vehicle rather than detailed travel coordinates. For the second track, the RUFTF proposed a law-based solution whereby the task force recommended the state legislature enact legislation prohibiting anyone connected with a state agency from accessing a GPS device to locate passenger vehicles either in real-time or by their travel history.

Oregon's first stage (2001-2007). The first Oregon distance charge pilot program deployed the RUFTF recommendation for the technology-based privacy solution by using a "thick client" device to travel data transmission. The deployed think client device used GPS coordinates to identify a pre-defined zone for travel and used the vehicle's speed sensor to produce the total miles driven during a period for purposes of calculating the distance charge. After making the calculation, the specific travel data were erased. Thus, there was neither transmission nor storage of vehicle travel locations. With this

technology, Oregon DOT hoped to obviate, by design, the system's ability to track a vehicle.

By all accounts, ODOT's technology solution worked as desired by effectively limiting exposure of precise travel information. The public, however, was not persuaded. As the 2007 pilot program report observes, "Many opponents of using GPS signals for road user charging argue that this is the first step towards complete government acquisition of private travel data." In its 2007 pilot report, ODOT noticed a trust issue: "When ODOT explains its efforts to protect citizen privacy, most citizens release their anxiety but with the caveat, 'As long as it's true.'"

Oregon's second stage (2010-2015). ODOT and the RUFTF learned from the negative public and media reactions to its first distance charge pilot that a technology-solution alone would not mollify generally held privacy concerns over use of GPS data. The emphasis shifted away from a technology solution to administrative and legal solutions.

During deliberations on RUC legislation in 2010, RUFTF proposed a two-pronged strategy. First, the payers of a RUC should have the option to choose non-location-aware technology for reporting travel data, thus removing the functional ability to collect location information. Secondly, the legislature should enact legal prohibitions and data management requirements to protect personally-identifiable information held by a government agency or a private entity for the purpose of collecting a RUC.

In a second, smaller demonstration in 2012-13, with eight state legislators participating, ODOT offered the choice of location-based reporting or non-location-based reporting. The success of the second pilot led to the passage of Senate Bill 810 in 2013 enacting a voluntary, operational per-mile RUC program that included not only a non-location reporting option but also privacy protection provisions negotiated with the American Civil Liberties Union, a privacy watchdog group.

Privacy provisions of Oregon's RUC Program. Oregon's per-mile RUC program legislation requires a non-location aware distance reporting option to allow participating motorists to elect not to have their travel patterns reported. Importantly, the legislation further declares personally identifiable information as confidential and establishes a prohibition from disclosing personally identifiable information obtained to collect a RUC to anyone other than the registered owner of a vehicle subject to the RUC or those involved with collecting travel data and the charge. The law applies the nondisclosure requirement

to the authorized agency (ODOT) and certified service providers involved in collection of travel data or administration to collect the charge and limits disclosure to information necessary to fulfill the respective recipient's function in the RUC program.

The law set forth an exception to this nondisclosure prohibition for police officers pursuant to a court order based on probable cause in a criminal investigation. Another exception is for an entity expressly approved to receive the information by the registered owner or lessee of the vehicle.

The law defines personally identifiable information as "any information that identifies or describes a person." The law then lists information and data that qualify, such as travel pattern data, but indicates that the definition is not limited to that list.

The law defines certified service providers as entities that have entered into an agreement with the authorized agency (ODOT) to collect metered use data and the per-mile RUC. There is no requirement that certified service providers must come from the private sector.

Oregon's RUC privacy law requires destruction of location and daily metered use data records, a subset of personally identifiable information, not later than 30 days after completion of the later of payment processing, dispute resolution, or a noncompliance investigation. There are exceptions allowing information stripped of its identifying qualities to be aggregated and used in traffic management and research and for monthly summaries of metered use by subject vehicles.

The law authorizes a certified service provider to retain location and daily metered use data records upon obtaining the consent of the registered owner or lessee of the subject vehicle. This consent exception does not apply to the authorized agency.

ODOT added more detail to the privacy protection law by administrative rule, including definitions for the following terms,

- Personally identifiable information does not include anonymized information or anonymized aggregated information.
- Anonymized information means information that does not identify or describe a person.

- Anonymized aggregated information means aggregated information accumulated in a way that preserves the anonymity of the persons participating in the RUC program, and does not identify or describe a person or create travel pattern data.
- Travel pattern data means location and daily metered use of a subject vehicle and data that describes a person's travel habits in sufficient detail that the person becomes identifiable either through the data itself or by combining publicly available information with the data.
- Non-compliance investigation means an investigation by the authorized agency to determine if, and to what extent, any person, including but not limited to a RUC payer, is in compliance with the statutory provisions and associated administrative rules.
- Express approval means active approval, either electronic or on paper, by a payer of RUC that identifies the entity which personally identifiable information will be shared.
- Consent means voluntary agreement given to retain location and daily metered use beyond the period required by law.

The administrative rules created the following rights for those owning or leasing a vehicle subject to the RUC with the requirement that the authorized agency and certified service provider respond to requests for exercise of these rights within five business days.

- The right to inquire about the nature, accuracy, status and use of and the right to examine the personally identifiable information or a reasonable facsimile thereof.
- The right to request correction of personally identifiable information upon provision of reasonable evidence that the information has errors or has changed.
- The right to erasure of the location and daily metered use data that has not been destroyed within the required period of time.

The following list constitutes the potentially relevant privacy protection provisions *not* included in the Oregon privacy protection law for RUC data.

1. The form that personal information must be kept.
2. The form of express approval.

3. What happens when express approval provisions are violated.
4. The right to withdraw express approval.
5. Whether a certified service provider may condition performance of duties on receiving express approval for sharing personal data with others.
6. Providing information relating to rights pertaining to personal information.
7. Providing information upon request and how the information is provided.
8. Whether consent should be required for a certified service provider to use personally identifiable information for other services beyond collection of a RUC.
9. Prohibition of discriminatory actions against persons exercising their rights.
10. Requirements for appropriate security measures.
11. Requirements for notification of a breach of security related to personally identifiable information.
12. Requirement for a certified service provider to appoint a specific person responsible for protection of personally identifiable information.
13. Establishment of certification mechanisms for certified service providers to demonstrate compliance with this privacy protection law.
14. Judicial and administrative remedies.
15. Preemption of local law.
16. Prohibition of attempts to waive this privacy protection law.
17. Requirements for anonymization of road usage charge information and data.
18. Requirements for maintaining a record of access to personally identifiable information.
19. Requirement for certified service providers to establish, publish and adhere to an internal usage and privacy policy available in writing.

California

The California Legislature passed Senate Bill 1077 in August 2014 directing the California State Transportation Agency (CalSTA) to conduct a pilot program demonstrating a system for charging by distance traveled. The legislature placed particular focus on protecting privacy during operation of the pilot program.

Statutory protection of privacy. Senate Bill 1077 declared that any exploration of RUC must take privacy implications into account and, specifically, that travel locations or patterns shall not be required to be reported to the state and, further, that technical

safeguards must protect personal information. The legislature directed empanelment of a technical advisory committee to consider the necessity of protecting all personally identifiable information used in reporting highway use to public and private agencies with an emphasis on protecting location data, to ensure protection of individual privacy rights under the California Constitution.

The legislature directed that the pilot design itself reflect privacy protection as a policy priority. The pilot program would analyze alternative means of collecting road usage data, including at least one means not reliant on electronic vehicle location data, while also collecting a minimum amount of personal information including location-aware information. To protect data integrity and safeguard privacy, the pilot would have processes for collection, management, storage, transmission, and destruction of data. The legislature directed that for all personal information or data collected during the pilot program, the state government not disclose, distribute, make available, sell, access, or provide such information for any purpose other than the pilot program, except for certain legal purposes involving a court order, subpoena, or warrant, or aggregated information, with all personal information removed, for purposes of academic research.

TAC privacy protection principles. In early 2015, the California Transportation Commission appointed the Technical Advisory Committee (TAC) to advise the California Department of Transportation on issues pertaining to a RUC pilot program, including protection of privacy. The commission appointed two individuals of prominence in the privacy protection arena to the TAC.

The importance of the protection of personal information and data generated from pilot program arose at the TAC's first meeting. Later, in July 2015, the TAC recommended the following privacy principles for application in the pilot but also generally if an operational program implementation occurred. The TAC used these principles to develop its Road Charge Pilot Program Privacy Policy.

1. The Road Charge system must at all time recognize and respect an individual's interests in privacy and information use pursuant to Section 1 of Article I of the California Constitution.
2. The Road Charge system must offer motorists a time-based system of paying for road use, as an alternative payment method for individuals concerned about disclosing their mileage driven.

3. The Road Charge system must allow motorists choice in how mileage will be reported.
4. The Road Charge system must be designed, implemented and administered in a manner transparent to the public and to individual motorists.
5. The Road Charge system must comply with applicable federal and state laws governing privacy and information security.
6. Personal information required for the Road Charge system must not be disclosed to any persons or entities without motorists' consent, specific statutory authority authorizing disclosure, appropriate legal process, or emergency circumstances as defined in law.
7. The Road Charge system shall not collect information beyond what is needed to properly calculate, report and collect the road charge, unless the motorist provides his or her consent.
8. Road Charge system data retained beyond the period of time necessary to ensure proper mileage account payment must have all personal information removed, and may only be used for public purposes (i.e., improve the safety and efficiency of the traveling public).
9. Motorists who choose to release personal information must provide their consent in a clear, unambiguous and written manner.
10. The Road Charge system must not require use of specific locational information, including specific origins or destinations, travel patterns or times of travel.
11. The Road Charge system must allow motorists an opportunity to view all personal data being collected and stored to ensure only data required for proper accounting and payment of road charges is being collected and retained.
12. The Road Charge system must investigate all potential errors identified by motorists and make all corrections to ensure road charge records remain accurate.

California pilot program privacy protection

The California Road Charge Pilot Program (2016-17) operationalized the California Road Charge Privacy Principles. The state made evident its commitment to the privacy principles by declaring adherence to them in the pilot program participant agreement and

including them as an attachment. Throughout the operation of the nine-month Road Charge Pilot Program, the state adhered to the privacy protections and, at the conclusion of the pilot, destroyed data in accordance with its requirements. The authorized agency also fulfilled several requests for aggregate pilot data in accordance with both state law (Senate Bill 1077) and the adopted principles.

Washington: the WA RUC Pilot Program privacy protection

For the Washington Road Usage Charge Pilot Program (2018), the Washington Transportation Commission applied a privacy policy similar to the one applied in California but identifying the personal information that would be collected and protected as well as limiting scope for which the personal information would be applied. This privacy policy offered the right for participants to inspect their information and records and prompt corrections and provide that location-aware reporting and services are optional.

APPENDIX D: GENERAL PRIVACY PROTECTION LAWS

I. United States

As stated above, the United States does not have any general privacy protection law at the federal level except for an inference in the U.S. Constitution stated in case law of the Supreme Court determined on a case-by-case basis and therefore not specific. Residents of a state cannot rely upon Supreme Court case law to understand how information and data obtained during collection of a RUC will be protected. To reassure residents of a state on this issue, a state legislature or Congress must enact a statute.

State law

Absent a federal directive for general protection of privacy data and information, any policy enactments protecting privacy for road usage charge data must come from the states.

According to the National Conference of State Legislatures, only ten states have provisions in their state constitutions directly protecting privacy.

- Alaska: The right of the people to privacy is recognized and shall not be infringed. Article I, section 22.
- Arizona: No person shall be disturbed in his private affairs, or his home invaded, without authority of law. Article II, section 8.
- California: All people are by nature free and independent and have inalienable rights. Among these are … pursuing and obtaining … privacy. Article I, section 1.
- Florida: Every natural person has the right to be let alone and free from governmental intrusion into the person's private life … Article I, section 23.
- Hawaii: The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. And further, the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and invasions of privacy shall not be violated … Article I, sections 6 and 7.
- Illinois: The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches of privacy or

interceptions of communications by eavesdropping devices or other means. Article I, section 6.

- Louisiana: Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches or invasions of privacy. Article I, section 5.
- Montana: The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest. Article II, section 10.
- South Carolina: The right of the people in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated … Article I, section 10.
- **Washington: No person shall be disturbed in his private affairs, or his home invaded, without authority of law. Article I, section 7.**

These constitutional provisions apply to government action. Whether the protections in these state constitutions extend to actions of non-governmental entities holding personal data or information is unknown. Also unknown are any duties inferred from these protections. For any legal certainty about the protection of privacy, state legislatures must enact legislation.

For example, the California Legislative Assembly augmented the state's constitutional privacy protection provision by enactment of the California Consumer Privacy Act and approval by the state's governor on June 28, 2018. The California Consumer Privacy Law primarily focuses on imposing requirements on businesses and rights to consumers with respect to consumer data rather than restricting or directing the actions of government.

The California privacy law grants consumers a right to disclosure of personal information that a business collects about the consumer, the sources from which it came, the purposes for collecting or selling the information, and the categories of third parties with which the information is shared. Specifically, the law, among other things, does the following:

- Right to disclosure. Grants a consumer a right to request disclosure of the categories and specific pieces of personal information that a business collects about the consumer, the categories of sources from which that

information is collected and requires a business to disclose the information and the purposes for which it is used.

- Right to deletion. Grants a consumer the right to request deletion of personal information and requires the business to delete upon receipt of a verified request.
- Rights when personal information is sold. Grants a consumer a right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of 3rd parties to which the information was sold or disclosed and requires a business to provide this information in response to a verifiable consumer request.
- Right to opt out. Authorizes a consumer to opt out of the sale of personal information by a business and prohibits the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer's data.
- Prohibits selling personal information of consumer under age 16. Prohibits a business from selling the personal information of a consumer under 16 years of age, unless affirmatively authorized, as specified, to be referred to as the right to opt in.
- Consumer requests. Prescribes requirements for receiving, processing, and satisfying requests from consumers.
- Personal information definition. Defines "personal information" with reference to a broad list of characteristics and behaviors, personal and commercial, as well as inferences drawn from this information.
- Prohibits restriction of compliance. Prohibits restriction of the ability of the business to comply with federal, state, or local laws, among other things.
- Enforcement. Provides for its enforcement by the Attorney General and provides a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's non-encrypted or non-redacted personal information.
- Attorney General opinion on compliance. Authorizes a business, service provider, or 3rd party to seek the Attorney General's opinion on how to comply with its provisions.

- Voids waiver. Voids a waiver of a consumer's rights under its provisions.
- Takes effect on January 1, 2020.

II. European Union General Data Protection Regulation (2018)

One month before the California Consumer Privacy Act was approved, the European Union implemented the General Data Protection Regulation (GDPR) on May 25, 2018. The stated purposes of the GDPR are (1) protection of fundamental rights and freedoms of natural persons regarding the processing of their personal data and their right to protection of personal data, and (2) free movement of personal data within the European Union.

The comprehensiveness and reach of the EU's GDPR renders this regulation relevant for consideration in development of a model privacy policy framework for distance charging in the United States. The EU's GDPR is far-reaching and covers some data processing not relevant to a distance charge enacted in the United States. As such, the following description of the essential GDPR provisions only summarizes some of the potentially relevant portions of the regulation.

Description of EU GDPR essential provisions

The GDPR protects personal data which means information related to identified or identifiable natural person. The GDPR applies to the processing of personal data by a controller or processor, wholly or partially by automated means (or, other means, if part of a filing system), where activities relate to the offering of goods or services irrespective of payment. A controller means a natural or legal person which determines the purposes and means of processing personal data. A processor means a natural or legal person which possesses personal data on behalf of the controller.

This regulation establishes principles for processing of personal data. These principles require that personal data shall be

- Processed lawfully, fairly and in a transparent manner;
- Collected and processed only for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to the purposes;
- Accurate and kept up to date and, if not, erased;
- Kept in a form which permits identification of data subjects no longer than necessary for the purposes; except that personal data may be kept for

longer periods for archiving in the public interest, scientific or historical research or statistical purposes subject to storage limitation; and
- Processed in a manner that ensures appropriate security of personal data, using appropriate technical or organizational measure.

The controller is responsible for compliance with these principles.

Data processing is considered lawful when the data subject has given consent to processing of personal data for specific purpose(s) and processing is necessary for:

- performance of the agreement;
- compliance with a legal obligation;
- protect vital interests of data subject or natural person;
- performance of task in the public interest; and
- legitimate interests pursued by controller (but not public authorities), except where overridden by interests of fundamental rights and freedoms of data subject.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or clear affirmative action signifies agreement to the processing of personal data related to the data subject. If in writing, the request for consent must be clearly distinguishable, intelligible and easily accessible in clear and plain language. If this provision is infringed, the consent will not be binding.

Data subject has right to withdraw consent at any time. Withdrawal of consent shall not affect lawfulness of consent given before withdrawal provided data subject was informed thereof. It shall be as easy to withdraw as give consent.

The GDPR established many rights for the data subject.

- Transparency of information related to rights. The controller shall provide information related to rights pertaining to personal data in writing, or where appropriate, by electronic means, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The controller shall facilitate the exercise of these rights and shall not refuse to act upon the request of a data subject unless the controller demonstrates an inability to identify the data subject. The controller shall provide information upon a

request for exercise of rights pertaining to personal data without undue delay and no longer than one month or receipt of request. Where request is made by electronic means, the information can be provided by electronic means. The information may be provided orally if requested by the data subject.

- Providing information related to identity and purpose. When personal data related to a data subject are obtained, the controller shall provide the data subject with the following information free of charge:
  - Identity and contact details of the controller;
  - Contact details of the data protection officer;
  - Purposes of and legal basis for the personal data processing;
  - Any legitimate interests pursued by the controller or third parties in collecting the personal data
  - Recipients, or categories of recipients, of the personal data, if any,
  - Whether the controller intends to transfer personal data internationally and reference to suitable safeguards and the means to obtain copy of them.
- Providing information related to personal information. At the time when personal data are obtained from the data subject, the controller shall provide the data subject the following information free of charge and in standard icons to give in an easily visible, intelligible and clearly legible manner, to ensure fair and transparent processing:
  - The period of storage or criteria to determine that period;
  - Existence of the right to request access to and rectification or erasure of personal data or restriction of processing or object to processing and the right to portability;
  - The existence of right to withdraw consent at any time without affecting the lawfulness of the processing on the prior consent;
  - The right to lodge a complaint with a supervisory authority;
  - Whether the provision of personal data is a statutory or contractual requirement, or necessary to enter into a contract, and whether the data subject is obliged to provide personal data and possible consequences of failure to do so;
  - The existence of automated decision-making, including profiling, and meaningful information related to it.

- Right of access to personal information. The data subject has the right to obtain confirmation from controller as to whether his/her personal data is being processed and access to that data and the following:
  - Purposes of the processing;
  - Categories of personal data concerned;
  - Recipients, or categories of recipients, of the personal data, if any,
  - The envisaged period for which the personal data will be stored or the criteria for determining that period
  - Existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of the personal data;
  - The right to lodge a third-party complaint with a supervising authority;
  - Where personal data are not collected from the data subject, any available information on the source;
  - The existence of automated decision-making, including profiling, and meaningful information related to it.
- Right to rectification. The data subject has the right to rectification of inaccurate personal data without undue delay or to have incomplete personal data completed.
- Right to erasure (right to be forgotten). The data subject has the right to erasure of personal data without undue delay and the controller has the obligation to erase personal data without undue delay where one of the following grounds applies:
  - The personal data are no longer necessary for the purpose of the collection;
  - The data subject withdraws consent on which processing is based;
  - The personal data have been unlawfully processed;
  - Compliance with a legal obligation is necessary;
  - Personal data were collected for information society services.

The right of erasure shall not apply to the extent processing is necessary:

- For exercising right of freedom of expression and information;
- Compliance with a legal obligation;
- Reasons of public interest in public health;
- Archiving purposes in the public interest, scientific, historical or statistical purposes;

- Establishment, exercise or defense of legal claims.

Notification obligation. Controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to which personal data were disclosed and inform data subject about recipients, if requested.

- Right to portability. The data subject has right to receive personal data provided to a controller in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller without hindrance where:
  - Processing is based on consent;
  - Processing is carried out by automated means.
- Right to object. Data subject shall have right to object at any time to processing of personal data which is based on carrying out a task in the public interest or exercise of controller's official authority or pursuits of legitimate interests. Controller shall no longer process the personal data unless controller demonstrates compelling legitimate grounds for processing sufficient to override interests, rights and freedoms of data subject or for establishment, exercise or defense of legal claims. Data subject shall have the right at any time to object to use of personal data for direct marketing purposes, including profiling, and those data will no longer be used for those purposes.

Security. The controller shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of destruction, loss, alteration, unauthorized disclosure of or access to personal data, including the following:

- Pseudonymization and encryption of personal data;
- Ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Ability to restore availability and access to personal data in a timely manner in event of an incident.

Data Protection Officer. The GDPR established a regimen for management of data processing of personal information and rights of the data subject. Within the regimen is designation of a data protection officer by the controller and processor in any case where:

- Processing is carried out by public authority or body;
- Core activities of controller or processor consist of processing operations which, by their nature, require regular and systematic monitoring of data subjects;
- Core activities of control or processor consist of processing on a large scale of special categories of data relating to racial or ethnic origin, public opinions, religious or philosophical beliefs, trade union membership, and processing of genetic data or biometric data or uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation or personal data relating to criminal convictions or offenses.

The GDRP assigns special tasks for the data protection officer.

Remedies. The GDPR establishes many rights and remedies pertaining to violations.

- Right to lodge complaint with a supervisory authority;
- Right to effective judicial remedies;
- Representation of data subject.
- Rights to compensation and liability.
- Administrative fines.
- Penalties. Development of privacy protection policies for U.S. RUC programs

WA RUC

APPENDIX E: COMPARISON OF SELECTED PRIVACY LAWS WITH MODEL PRIVACY POLICY

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
I. GENERAL PROVISIONS				
Stated Purpose	Protection of fundamental rights and freedoms of natural persons with regard to processing of personal data and their right to protection of their personal data and the free movement of personal data within the EU. **A1.1.2.3.**	To further the right of privacy in the California Constitution and to supplement existing laws relating to consumer's personal information by giving consumers an effective way to control their personal information. **Section 3, 1798.175.**	A specific purpose is not stated but the statute implies that its purpose is protection of personally identifiable information related to collection of a per-mile road usage charge from disclosure. **ORS 319.915.**	The is law protects personal information related to collection of per-mile road usage charges from disclosure. A ***Road Usage Charge Program*** is a statutory program, supported by administrative rules, for collecting road usage charges for metered use of a subject vehicle on the highways of the state.
Protected data	***Personal data*** means information related to an identified or identifiable natural person, a "***data subject***." **A4(1).**	***Personal information*** means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly with a particular consumer or household, including the following: • Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers; • Any categories of personal information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, drivers license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card	***Personally identifiable information*** means information that identifies or describes a person that is obtained or developed in the course of reporting metered use by a subject vehicle or for providing administrative services related to the collection of road usage charges, including but not limited to, the person's travel pattern data, per-mile road usage charge account number, address, telephone number, electronic mail address, driver license or identification card number, registration plate number, photograph, recorded images, bank account information and credit card number but does not include anonymized information or anonymized aggregated information. **ORS 319.915(1)(b); OAR 731-090-0010(23).** **Anonymized information** means information that does not identify or	***Personal information*** means information or data that identifies, relates to or describes a person that is obtained or developed in the course of reporting metered use by a subject vehicle or for providing administrative services related to the collection of road usage charges. ***Personal information*** does not include anonymized aggregated information. ***Anonymized information*** means information that cannot reasonably

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	number, debit card number, or any other financial information, medical information, or health insurance information. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records; • Characteristics of protected classification under California or federal law; • Commercial information, including records of personal property, products of services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; • Biometric information; • Internet or other electronic network activity information, including browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement; • Geolocation data; • Audio, electronic, visual, thermal, olfactory, or similar information; • Professional or employment-related information; • Education information, defined as information that is not publicly available personally identifiable information; • Inferences drawn from any of the information identified to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. **Section 3, 1798.140(o)(1).** ***Personal information*** does not include publicly available information that is lawfully made available from federal, state, or local government records. Information is not ***publicly available*** if,	describe a person. OAR 731-090-0010(2). ***Anonymized aggregated information*** means aggregated information accumulated in a way that preserves the anonymity of the persons participating in the Road Usage Charge Program, and does not identify or describe a person or create travel pattern data. **OAR 731-090-0010(3).** ***Travel pattern data*** means location and daily metered use of a subject vehicle and data that describes a person's travel habits in sufficient detail that the person becomes identifiable either through the data itself or by combining publicly available information with the data. **OAR 731-090-0010(32).**	identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person, provided a service provider has implemented technical safeguards and processes that prohibit re-identification of the person, processes that prevent inadvertent release of the information and makes no attempt to re-identify the information. ***Anonymized aggregated information*** means aggregated information accumulated in a way that preserves the anonymity of the persons reporting metered use by a subject vehicle related to collection of a road usage charge and does not identify or describe a person or create travel pattern data. ***Travel pattern data*** means location and daily metered use data of a subject vehicle and data that describes a person's travel habits in sufficient detail that the person becomes identifiable either through the data itself or by combining publicly available information with the data.

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• it is biometric information collected by a business about a consumer without the consumer's knowledge; • data is used for a purpose that is not compatible with the purpose for which the date is maintained and made available in the government records or for which it is publicly maintained; • consumer information that is de-identified or aggregate consumer information. **Section 3, 1798.140(o)(2).** ***Aggregate consumer information*** means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device but does not mean one or more individual consumer records that have been deidentified. **Section 3, 1798.140(a).** A ***device*** means physical object that is capable of connecting to the Internet, directly or indirectly, or to another device. **Section 3, 1798.140(j).** ***Deidentified*** means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided a business has implemented technical safeguards and processes that prohibit reidentification of the consumer, processes that prevent inadvertent release of deidentified information and makes no attempt to reidentify the information. **Section 3, 1798.140(h).** ***Unique identifier*** or ***unique personal identifier*** means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services,		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
		including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. **Section 3, 1798.140(x).** ***Probabilistic identifier*** means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information. **Section 3, 1798.140(p).**		
Material Scope	Applies to the processing of personal data wholly or partly by automated means or other means if part of a filing system. **A2.1.2.3.4.** ***Processing*** means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction. **A4(2).** A ***filing system*** means any structured set of personal data which are accessible according to specific criteria. **A4(6).**	Applies to the ability of individuals to control the use, including the sale, of their personal information. **Section 2(a).** ***Processing*** means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means. **Section 3, 1798.140(q).**	The registered owner or lessee of a subject vehicle shall report the metered use by that vehicle and pay the per-mile road usage charge due for metered use of the highways in the state. **ORS 319.885(1)(a)(b) & ORS 319.920(1).** ***Registered owner*** means a person, other than a vehicle dealer, that is required to register a motor vehicle in Oregon. **ORS 319.883(4).** ***Lessee*** means a person that leases a motor vehicle that is required to be registered in Oregon. **ORS 319.883(2)** ***Subject vehicle*** means a motor vehicle that is the subject of an application to volunteer to pay the per-mile road usage charge for metered use by the vehicle. **ORS 319.883(5).**	This policy applies to processing of personal information reported by a registered owner or lessee wholly or partly by automated or other means for purposes of paying a per-mile road usage charge for metered use by a subject vehicle of the highways of the state. ***Processing*** means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means. ***Registered owner*** means a person, other than a vehicle dealer, that is required to register a motor vehicle in the state. ***Lessee*** means a person that leases a motor vehicle that is required to be registered in the state.

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
				Subject vehicle means a motor vehicle that is the subject of an application to volunteer to pay the per-mile road usage charge for metered use by the vehicle.
Territorial Scope	Applies to the processing of personal data by a controller or processor, whether established in the EU or not, where activities relate to the offering of goods or services irrespective of payment. **A3.1.2.3.** A ***controller*** means the natural or legal person, public authority, agency or other body which determines, either alone or jointly, the purposes and means of processing personal data. **A4(7)** A ***processor*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller. **A4(8).**	It is the intent of the state legislature to further Californian's right to privacy by giving consumers an effective way to control their persona information. **Section 2(i).**	Applies to personally identifiable information used for reporting metered use of subject vehicles on the highways of the state of Oregon or for administrative services related to the collection of the per-mile road usage charge established in Oregon. **ORS 319.915(2).**	This policy applies to the processing of personal information by a commercial or government entity, whether established in the state or not, where activities relate to collection of a per-mile road usage charge irrespective of payment.
II.PRINCIPLES				
Principles related to processing of personal data	Personal data shall be: a: Processed lawfully, fairly and in a transparent manner; b: Collected and processed only for specified, explicit and legitimate purposes; c: Adequate, relevant and limited to the purposes; d: Accurate and kept up to date and, if not, erased; e: Kept in a form which permits identification of data subjects no longer than necessary for the purposes; except that personal data may be kept for longer periods for archiving in the public interest,		Personally identifiable information used for reporting metered use or for administrative services related to the collection of the per-mile road usage charge is confidential and is a public record exempt from disclosure. **ORS 319.915(2).** The DOT or a certified service provider may not disclose personally identifiable information used or developed for reporting metered use by a subject vehicle or for administrative services related to collection of per-mile road usage charges to any person, except:	*[If a state's public records laws grant public access to driving records,]* personal information used for reporting metered use or for administrative services related to the collection of the per-mile road usage charge is confidential and is a public record exempt from disclosure. Information collected for use in a Road Usage Charge Program shall be accurate, relevant and collected and processed in a transparent manner only for use in collecting a per-mile road usage charge from a registered owner of lessee of a subject vehicle. The personal

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
scientific or historical research or statistical purposes subject to storage limitation; f: Processed in a manner that ensures appropriate security of personal data, using appropriate technical or organizational measure. **A5.1.** The controller shall be responsible for compliance with the above principles. The controller is the natural or legal person, public authority, agency or other body which determines the purposes and means of processing personal data. **A5.2; A4(7)**		• the registered owner or lessee; • a financial institution, for the purpose of collecting per-mile road usage chargers owed; • employees of the DOT; • a certified service provider; • a contractor for a certified service provider, but only to the extent the contractor provides services directly related to an agreement with the DOT; • an entity expressly approved to receive the information by the registered owner or lessee of the subject vehicle; • a police officer pursuant to a valid court order based on probable cause and issued at the request of a federal, state or local law enforcement agency in an authorized criminal investigation involving the person to who the requested information pertains. **ORS 319.915(3)(a).** Disclosure of personally identifiable information is limited to the information necessary to the respective recipient's function in regard to collection of per-mile road usage charges. **ORS 319.915(3)(b).**	information shall be kept in a form which permits identification of the subject vehicle and its registered owner of lessee no longer than necessary and processed in a manner that ensures appropriate security, using appropriate technical or organizational measures. No person or entity involved with collection of a per-mile road usage charge may disclose personal information used of developed for reporting metered use by a subject vehicle or for administrative services related to collection of per-mile road usage charges to any person, except to the following recipients limited to the information necessary to the respective recipient's function in collecting per-mile road usage charges: • the registered owner or lessee; • a financial institution, for the purpose of collecting per-mile road usage chargers owed; • employees of the DOT; • a service provider; • a contractor for a service provider, but only to the extent the contractor provides services directly related to an agreement with the DOT; • an entity expressly approved to receive the information by the registered owner or lessee of the subject vehicle; • a police officer pursuant to a valid court order based on probable cause and issued at the request of a federal, state or local law enforcement agency in an authorized criminal investigation involving the person to who the requested information pertains.

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
			An authorized agency or service provider that accesses or provides access to personal information shall maintain a record of that access. The access control log shall include: • Date and time the information is accessed; • The data elements used to query the road usage charge database or system; • The person accessing the personal information; • The purpose for accessing the information.
	A ***service provider*** means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business. **Section 3, 1798.140(v).**	A ***certified service provider*** means an entity that has entered into an agreement with the DOT for reporting metered use by a subject vehicle or for administrative services related to the collection of per-mile road usage charges and authorized employees of the entity. **ORS 319.915(1)(a).**	A ***service provider*** means an entity that has entered into an agreement with the authorized agency for reporting metered use by a subject vehicle or for administrative services related to the collection of per-mile road usage charges and authorized employees of the entity. The state should appoint a state agency to act as a service provider as an alternative to contracted service providers.
		Express approval means active approval, either electronic or on paper, by a payer of road usage charges that identifies the entity which personally identifiable information will be shared. **OAR 731-090-0010(9).**	***Express approval*** means active approval, either electronic or on paper, by a payer of road usage charges that identifies the entity which personal information will be shared. The request for express approval must be clearly distinguishable, intelligible and easily accessible in clear and plain language. If

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
				this provision is infringed, the express approval will not be binding. The person providing personal information has right to withdraw express approval at any time. Withdrawal of express approval shall not affect lawfulness of express approval given before withdrawal provided the person was informed thereof. It shall be as easy to withdraw as give express approval. ***Authorized agency*** means a government agency assigned the responsibility and given the authority to implement and operate the Road Usage Charge Program.
Principles for lawful processing of data	Data processing is lawful when the data subject has given consent to processing of personal data for specific purpose(s) and processing is necessary for: • performance of the agreement; • compliance with a legal obligation; • protect vital interests of data subject or natural person; - performance of *task* in the public interest; • legitimate interests pursued by controller (but not public authorities), except where overridden by interests of fundamental rights and freedoms of data subject. **A6.1.** The basis for processing shall be determined by law or by necessity in performance of a task carried out in the public interest or the exercise of official authority vested in the controller. **A6.3.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or clear affirmative action signifies agreement to the processing of personal data related to the data subject. **A3(11).**			***Consent*** means any freely given, specific, informed and unambiguous indication by a registered owner or lessee of a subject vehicle by a clear affirmative action to select a mileage reporting method signifies agreement to collection and processing of metered use data for use in assessing a per-mile road usage charge.
	Where processing is not based on the data subject's consent or on EU or member state law, controller shall take into account: (a) any link between purposes for gathering personal data and purposes for intended further processing; (b) context for collection of personal data, in particular relationship between data subjects and controller; (c) natural of personal data; (d) possible consequences of further processing; (e) existence of appropriate safeguards, including encryption or pseudonymization. **A6.4.** ***Pseudonymization*** means processing of personal data in such a manner that the personal data can no longer be attributed to specific data subject without additional information. **A3(5).**	***Pseudonymize*** or ***pseudonymization*** means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer. **Section 3, 1798.140(r).**		
Principles: conditions for consent	For processing based on consent, controller must be able to demonstrate consent to processing of personal data was granted by data subject. **A7.1.**			
	If consent is written, the request for consent must be clearly distinguishable, intelligible and easily			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	accessible in clear and plain language. If this provision is infringed, the consent will not be binding. **A7.1.2.**			
	Data subject has right to withdraw consent at any time. Withdrawal of consent shall not affect lawfulness of consent given before withdrawal provided data subject was informed thereof. It shall be as easy to withdraw as give consent. **A7.3.**			Data subject has right to withdraw consent at any time. Withdrawal of consent shall not affect lawfulness of consent given before withdrawal provided data subject was informed thereof. It shall be as easy to withdraw as give consent.
	When assessing whether consent was freely given, utmost account shall be taken of whether performance of the contract is conditional on consent to processing of personal data that is not necessary to contract performance. **A7.4.**			
Principles: conditions applicable to child's consent	This law applies to processing of data for children at least 16 years old. **A8.1.2.3.**			
Principles: processing of special categories of personal data	Prohibits processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or genetic data, biometric data of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. **A9.1.**			
	Exceptions: if, • explicit consent is given for data processing for specified purposes; • processing is necessary under employment, social security and social protection law;			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• processing is necessary to protect vital interests of data subject or natural person where physically or legally incapable of giving consent; • processing is carried out for members of political, philosophical, religious or trade union if consent is given; • processing relates to personal data manifestly made public by data subject; • processing is necessary for establishment, exercise or defense of legal claims; processing is necessary for reasons for reasons of substantial public interest proportionate to the aim pursued, provided there are safeguards of fundamental rights and interests of the data subject; • processing is necessary for purposes of preventative or occupational medicine; • processing is necessary for reasons of public interest in the area of public health; • processing is necessary for archiving purposes in the public interest. **A9.2.**			
	Processing of revealing personal data is permissible under responsibility of a professional subject to the obligation of professional secrecy. **A9.3.**			
	Member states are allowed to establish further conditions and limitations with regard to processing genetic data, biometric data or data concerning health. **A9.4.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Principles: processing of personal data related to criminal convictions and offenses	Processing of personal data related to criminal convictions of offenses shall be carried out only under the control of an official authority. **A10.**			
Principles: processing not requiring identification	If the purposes for processing personal data do not (or no longer) require identification of a data subject, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject to comply with the GDPR. If the controller is able to demonstrate this non-obligation, the controller shall inform the data subject of this accordingly and the rights of rectification, erasure, restriction of processing, and notification thereof, and portability do not apply. **A11.**			
III.RIGHTS OF THE DATA SUBJECT				
Rights: transparency and modalities	The controller shall provide information related to rights pertaining to personal data in writing, or where appropriate, by electronic means, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information may be provided orally if requested by the data subject. **A12.1.**			The service provider shall provide information related to rights pertaining to personal information in writing, or where appropriate, by electronic means, in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information may be provided orally if requested by the data subject.
	The controller shall facilitate the exercise of these rights and shall not refuse to act upon the request of a data subject unless the controller demonstrates an inability to identify the data subject. **A12.2.3.**			The service provider shall facilitate the exercise of these rights and shall not refuse to act upon the request of a distance charge payer.

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	The controller shall provide information upon a request for exercise of rights pertaining to personal data without undue delay and no longer than one month or receipt of request. Period may be extended for up to two months taking into account complexity and number of requests provided controller informs data subject of the extension within one month of receipt of request along with reasons for the delay. Where request is made by electronic means, the information can be provided by electronic means. **A12.3.**			The service provider shall provide information upon a request for exercise of rights pertaining to personal information without undue delay and no longer than one month or receipt of request. Where request is made by electronic means, the information can be provided by electronic means.
	If controller does not take action on the request of the data subject, the controller shall inform the data subject without delay but no later than one month after receipt of the request of the reasons for not taking action and the possibility for lodging a complaint with a supervisory authority and seeking judicial remedy. **A12.4.** A ***supervisory authority*** means an independent public authority established by a member state of the EU pursuant to Article 51. **A3(21).**			If service provider does not take action on the request of the distance charge payer, the controller shall inform the distance charge payer without delay but no later than one month after receipt of the request of the reasons for not taking action and the possibility for lodging a complaint with a supervisory authority and seeking judicial remedy.
	Where controller has reasonable doubts concerning the identify of a natural person making the request pertaining to personal information, the controller may request additional information necessary to confirm identity of the data subject. **A12.6.**			
Information and access to personal data				
Rights: information to be provided where	When personal data related to a data subject are obtained, the controller			When personal information related to a distance charge payer are obtained, the service provider shall provide the

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
personal data are collected from data subject	shall provide the data subject with the following information free of charge: • identity and contact details of the controller; • contact details of the data protection officer; • purposes of and legal basis for the personal data processing; • any legitimate interests pursued by the controller or third parties in collecting the personal data • recipients, or categories of recipients, of the personal data, if any, • whether the controller intends to transfer personal data internationally and reference to suitable safeguards and the means to obtain copy of them. Where requests are manifestly unfounded or excessive, the controller may charge a reasonable fee taking into account administrative costs or refuse to act on the request. **A13.1; A12.5.**			distance charge payer with the following information free of charge: • identity and contact details of the service provider; • contact details of the data protection officer; • purposes of and legal basis for the personal data processing; • any legitimate interests pursued by the controller or third parties in collecting the personal data • recipients, or categories of recipients, of the personal data, if any.
	At the time when personal data are obtained from the data subject, the controller shall provide the data subject the following information free of charge (unless the requests is unfounded or excessive and demonstrated by the controller) and in standard icons to give in an easily visible, intelligible and clearly legible manner, to ensure fair and transparent processing: • the period of storage or criteria to determine that period; • existence of the right to request access to and rectification or erasure of personal data or restriction of processing or			At the time when personal information are obtained from the distance charge payer, the controller shall provide the distance charge payer the following information free of charge and in standard icons to give in an easily visible, intelligible and clearly legible manner, to ensure fair and transparent processing: • the period of storage or criteria to determine that period; • existence of the right to request access to and rectification or erasure of personal data or restriction of processing or object to processing and the right to portability;

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	object to processing and the right to portability; • the existence of right to withdraw consent at any time without affecting the lawfulness of the processing on the prior consent; • the right to lodge a complaint with a supervisory authority; • whether the provision of personal data is a statutory or contractual requirement, or necessary to enter into a contract, and whether the data subject is obliged to provide personal data and possible consequences of failure to do so; • the existence of automated decision-making, including profiling, and meaningful information related to it. **A13.2.**			• the existence of right to withdraw consent or express approval at any time without affecting the lawfulness of the processing on the prior consent; • the right to lodge a complaint with the DOT; • whether the provision of personal information is a statutory or contractual requirement, or necessary to enter into a contract, and whether the distance charge payer is obliged to provide personal data and possible consequences of failure to do so.
	Where the controller intends to further process personal data for another purpose, the controller shall provide the data subject prior to the further processing with information on that other purpose and other relevant information. **A13.3.**			
	The rights above do not apply where the data subject already has the information. **A13.4.**			
Rights: Information to be provided where personal data <u>not</u> obtained from data subject	Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information; • identity and contact details of the controller; • contact details of the data protection officer; • purposes of and legal basis for the personal data processing;	For a business that collects personal information about a consumer, the consumer shall have the right to request disclosure of, and a business that collects personal information about a consumer shall disclose to the consumer upon receipt of a verifiable consumer request, the following: • the categories of personal information the business has collected about the consumer;		

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
• any legitimate interests pursued by the controller or third parties in collecting the personal data • categories of personal data concerned • recipients, or categories of recipients, of the personal data, if any, • whether the controller intends to transfer personal data internationally and reference to suitable safeguards and the means to obtain copy of them. **A14.1.** The controller shall provide the data subject the following information free of charge (unless the requests is unfounded or excessive and demonstrated by the controller), and in standard icons to give in an easily visible, intelligible and clearly legible manner, to ensure fair and transparent processing: • the period of storage or criteria to determine that period; • existence of the right to request access to and rectification or erasure of personal data or restriction of processing or object to processing and the right to portability; • the existence of right to withdraw consent at any time without affecting the lawfulness of the processing on the prior consent; • the right to lodge a complaint with a supervisory authority; • from which source the personal data originate and whether it came from publicly accessible sources; • the existence of automated decision-making, including	• the categories of sources from which the personal information is collected; • the business or commercial purpose for collecting or selling personal information; • the categories of third parties with whom the business shares personal information; • the specific pieces of personal information it has collected about that consumer. **Section 3, 1798.110(a)(b).** A ***verifiable consumer request*** or ***verifiable request*** means a request made by a consumer, or on behalf of a consumer's minor child, or by a natural person registered with the Secretary of State who is authorized to act on behalf of the consumer, and that the business can reasonably verify pursuant to regulations adopted by the Attorney General. **Section 3, 1798.140(y).** A business that collects personal information about consumers shall disclose the following: • the categories of personal information the business has collected about the consumer; • the categories of sources from which the personal information is collected; • the business or commercial purpose for collecting or selling personal information; • the categories of third parties with whom the business shares personal information; • the specific pieces of personal information it has collected about that consumer. **Section 3, 1798.110(c).**		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	profiling, and meaningful information related to it. Where requests are manifestly unfounded or excessive, the controller may charge a reasonable fee taking into account administrative costs or refuse to act on the request. **A14.2; A12.5.**			
	The controller shall provide this information within a reasonable period after obtaining the personal data but at least within one month; and if the personal data are being used for communication with the data subject, the information shall be provided concurrent with the first communication; and for disclosures to other recipients, when the persona data are first disclosed. **A14.3.**			
	Where the controller intends to further process personal data for another purpose, the controller shall provide the data subject prior to the further processing with information on that other purpose and other relevant information. **A14.4.**			
	The rights above do not apply where: • the data subject already has the information; • provision of the information proves impossible or would involve a disproportionate effort, subject to conditions and safeguards for ensuring technical and organizational measures are in place, including data minimization and pseudonymization;			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• obtaining or disclosure is expressly laid out by the EU or member state law; • where personal data must remain confidential subject to an obligation of professional secrecy regulated by the EU or a member state. **A14.5.**			
Rights: access by data subject	Data subject has the right to obtain confirmation from controller as to whether his/her personal data is being processed and access to that data and the following: • purposes of the processing; • categories of personal data concerned; • recipients, or categories of recipients, of the personal data, if any, • the envisaged period for which the personal data will be stored or the criteria for determining that period • existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of the personal data; • the right to lodge a third-party complaint with a supervising authority; • where personal data are not collected from the data subject, any available information on the source; • the existence of automated decision-making, including profiling, and meaningful information related to it. **A15.1.**	A consumer shall have the right to request that a business that collects a consumer's personal information disclose the categories and specific pieces of personal information collected. The business shall provide the information to a consumer upon receipt of a verifiable consumer request. A business need not retain information collected for a single, one-time transaction, if such information is not sold or retained by the business or to re-identify or otherwise link information that is not maintained in a manger that would be considered personal information. **Section 3, 1798.100(a)(b)(c)(e).**	The registered owner or lessee of a subject vehicle has the right to inquire about the nature, accuracy, status and use of and the right to examine the personally identifiable information or a reasonable facsimile thereof. **OAR 731-090-0010(5)(a)(b).** The DOT or certified service provider shall respond to requests for inquiry or examination within five business days of receipt of the request. **OAR 731-090-0010(5)(e).**	A distance charge payer has the right inquire about the nature, accuracy, status and use of personal information and the right to examine the personally identifiable information, or a reasonable facsimile thereof, and the right to request from the service provider rectification or erasure of personal information, if held beyond the 30-day holding period, and the right to lodge a third-party complaint with the DOT. The service provider shall respond to requests for inquiry or examination within five business days of receipt of the request.
	Whether the personal data are transferred internationally, the data subject shall have the right to be			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	informed of appropriate safeguards. **A15.2.**			
	Controller shall provide a copy of personal data undergoing processing but may only charge a reasonable fee for additional copies. Requests made by electronic means may be responded to in kind. The right to obtain a copy shall not adversely affect the rights and freedoms of other. **A15.3.**	The business shall disclose and deliver the requested personal information free of charge. The information may be provided by mail or electronically and if so portably and in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business shall not be required to provide personal information to a consumer more than twice in a 12-month period. **Section 3, 1798.100(d).**		
Rights: rectification	The data subject has the right to rectification of inaccurate personal data without undue delay or to have incomplete personal data completed. **A16.**		The registered owner or lessee of a subject vehicle has the right to request corrections of personally identifiable information upon provision of reasonable evidence that the information has errors or has changed. **OAR 731-090-0010(5)(c).** The DOT or certified service provider shall respond to requests for corrections within five business days of receipt of the request. **OAR 731-090-0010(5)(e).**	The distance charge payer has the right to request rectification of personal information upon provision of reasonable evidence that the information has errors or has changed. The service provider shall respond to requests rectification within five business days of receipt of the request.
Right to erasure (right to be forgotten)	The data subject has the right to erasure of personal data without undue delay and the controller has the obligation to erase personal data without undue delay where one of the following grounds applies: • the personal data are no longer necessary for the purpose of the collection; • the data subject withdraws consent on which processing is based; • the personal data have been unlawfully processed;	A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. A business that collects personal information about consumers shall disclose, including the designated methods for submitting requests, the consumer's rights to request deletion of the consumer's personal information. A business that receives a verifiable request from a consumer to delete the consumer's personal information shall delete the information from its records and direct any service providers to	Not later than 30 days after completion of payment processing, dispute resolution for a single reporting period or a noncompliance investigation, whichever is latest, the DOT and certified service provider shall destroy records of the location and daily metered use of subject vehicles. **ORS 319.915(4).**	Not later than 30 days after completion of payment processing, dispute resolution for a single reporting period or a noncompliance investigation, whichever is latest, the service provider shall erase records of the location and daily metered use of subject vehicles. The data subject has the right to erasure of personal data without undue delay and the controller has the obligation to erase personal data without undue delay.

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• compliance with a legal obligation is necessary; • personal data were collected for information society services. **A17.1**.	delete the consumer's personal information from their records. **Section 3, 1798.105(a)(b)(c).** ***Designated methods for submitting requests*** means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under the California Consumer Privacy Law, and any new, consumer-friendly means of contacting a business, as approved regulations or otherwise by the Attorney General. **Section 3, 1798.140(i).**		
		A business or service provider shall not be required to comply with a deletion request if the information is necessary for the business or service provider to maintain the information in order to: • Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, ore reasonably anticipated within the context of as business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer; • Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity; • Debug to identify and repair errors that impair existing intended functionality; • Exercise free speech, ensure the right of another consumer to exercise his/her right to free speech, or exercise another right provided by law; • Comply with the California Electronic Privacy Act; • Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all	***Non-compliance investigation*** means an investigation by DOT to determine if, and to what extent, any person, including but not limited to a payer of road usage charges, is in compliance with the statutory provisions of the Road Usage Charge Program and associated administrative rules. Such investigations may include informal inquiries or a formal review of the relevant records and the mileage reporting method of the payer or manager of accounts to ascertain the extent of non-compliance, if any. **OAR 731-090-0010(17).** The registered owner or lessee of a subject vehicle has the right to erasure of the location and daily metered use data that has not been destroyed within the required period of time. **OAR 731-090-0010(5)(d).** The DOT or certified service provider shall respond to requests for erasure within five business days	***Non-compliance investigation*** means an investigation by the authorized agency to determine if, and to what extent, any person, including but not limited to a distance charge payer, is in compliance with the statutory provisions of the Road Usage Charge Program and associated administrative rules. Such investigations may include informal inquiries or a formal review of the relevant records and the mileage reporting method of the payer or manager of accounts to ascertain the extent of non-compliance, if any. The registered owner or lessee of a subject vehicle has the right to erasure of the location and daily metered use data that has not been destroyed within the required period of time. The service provider shall respond to requests for erasure within five business days of receipt of the request.

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent; • To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; • Comply with a legal obligation; • Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. **Section 3, 1798.105(d).**	of receipt of the request. **OAR 731-090-0010(5)(e).**	
		Exceptions: • Information retained in records may be retained, aggregated and used for purposes of traffic management and research after personally identifiable information has been removed. **ORS 319.915(4)(b)(A).** • Monthly summaries of metered use by subject vehicles may be retained in VIN Summary Reports. ***VIN summary report*** means a monthly report by DOT or certified service provider that includes a summary of all vehicle identification numbers of subject vehicles and associated total metered use during the month but not include location information. **ORS 319.915 (1)(c) and (4)(b)(C).** • A certified service provider may retain and use records of location and daily metered use	Exceptions: • Records accumulated as anonymized aggregated information may be retained and used for purposes of traffic management and research. • Monthly summaries of metered use by subject vehicles may be retained in VIN Summary Reports. ***VIN summary report*** means a monthly report by • service provider that includes a summary of all vehicle identification numbers of subject vehicles and associated total metered use during the month but not include location information. • A service provider may retain and use records of location and daily metered use of subject vehicles if the registered owner or lessee of the subject vehicle consents to the retention. Consent does not entitle the authorized agency to obtain or use the records or the information in

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
			of subject vehicles if the registered owner or lessee of the subject vehicle consents to the retention. Consent does not entitle the DOT to obtain or use the records or the information in the records. **ORS 319.915(4)(b)(B); OAR 731-090-0010(3).** ***Consent*** means voluntary agreement given to retain location and daily metered use beyond the period required by law. **OAR 731-090-0010(6).**	the records. Any records retained by authority of consent of the road usage charge payer shall be anonymized. ***Consent*** means voluntary agreement given to retain location and daily metered use beyond the period required by law.
	Where controller is obligated to erase personal data, controller shall take reasonable steps to inform controllers of the request for erasure. **A17.2.**			
	The right of erasure shall not apply to the extent processing is necessary: • for exercising right of freedom of expression and information; • compliance with a legal obligation; • reasons of public interest in public health; • archiving purposes in the public interest, scientific, historical or statistical purposes; • establishment, exercise or defense of legal claims. **A17.3.**			The right of erasure shall not apply to the extent processing is necessary for compliance with a legal obligation or establishment, exercise or defense of legal claims.
Right to restriction of processing	The data subject shall have the right to obtain restriction of processing where one of the following applies: • Accuracy of personal data is contested for the period enabling controller to verify accuracy; • Processing is unlawful and data subject opposes erasure;			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• Controller no longer needs personal data for purposes of processing but required by data subject for reasons related to legal claims; • Data subject objects to processing pending verification whether controller has legitimate grounds. **A18.1.**			
	Where processing is restricted, personal data shall only be restricted, other than for storage, with data subject's consent related to legal claims or for protection of rights of another natural or legal person or for reasons of public interest. **A18.2.**			
	Controller shall inform data subject before restriction of processing is lifted. **A18.3.**			
Notification obligation regarding rectification or erasure or restriction of processing	Controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to which personal data were disclosed and inform data subject about recipients, if requested. **A19.**			The service provider shall communicate any rectification or erasure of personal information to each recipient to which personal information were disclosed and inform distance charge payers about recipients, if requested.
Right to data portability	Data subject has right to receive personal data provided to a controller in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller without hindrance where: • Processing is based on consent; • Processing is carried out by automated means. **A20.1.**			A road usage charge payer has right to receive personal information provided to a service provider in a secure, structured, commonly used and machine-readable format and has the right to transmit that personal information to another service provider without hindrance. A road usage charge payer has the right to have personal information securely transmitted directly from one service provider to another where technically feasible.

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	Data subject has right to have personal data transmitted directly from one controller to another where technically feasible but this right shall not apply to processing necessary for carrying out public interest or exercise of official authority vested in controller nor adversely affect the rights of others. **A20.2.3.4.**			
Right to object	Data subject shall have right to object at any time to processing of personal data which is based on carrying out a task in the public interest or exercise of controller's official authority or pursuits of legitimate interests. Controller shall no longer process the personal data unless controller demonstrates compelling legitimate grounds for processing sufficient to override interests, rights and freedoms of data subject or for establishment, exercise or defense of legal claims. **A21.1.**			
	Data subject shall have the right at any time to object to use of personal data for direct marketing purposes, including profiling, and those data will no longer be used for those purposes. A21.2.3.	A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, shall disclose to the consumer: • the categories of personal information that the business collected about the consumer; • the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; • the categories of personal information that the business disclosed about the consumer for a business purpose. **Section 3, 1798.115(a).**		

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	A business that sells personal information about a consumer or that discloses a consumer's personal information shall disclose to that consumer: • the categories of personal information that the business collected about the consumer; • the categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; • the categories of personal information that the business disclosed about the consumer for a business purpose. **Section 3, 1798.115(b).** • A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose: • the category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact; • the category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact. **Section 3, 1798.115(c).** A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out. **Section 3, 1798.115(d).**		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Right to Opt Out and Right to Opt In		***Right to Opt Out***. A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. **Section 3, 1798.120(a).** A business that sells consumers' personal information to third parties shall provide notice to consumers that this information may be sold and that consumers have the right to opt out of the sale of their personal information. **Section 3, 1798.120(b).** A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information. **Section 3, 1798.120(c).** (1) Provide a clear and conspicuous link on the business' Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information. (2) Include a description of a consumer's rights along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in: (A) Its online privacy policy or policies if the business has an online privacy policy or policies.		

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	(B) Any California-specific description of consumers' privacy rights. (3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements related to the rights of disclosure, opt in, opt out and notice and how to direct consumers to exercise these rights. (4) For consumers who exercise their right to opt out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer. (5) For a consumer who has opted out of the sale of the consumer's personal information, respect the consumer's decision to opt out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information. (6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request. **Section 3, 1798.135(a).** Nothing in this law shall be construed to require a business to comply by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally. **Section 3, 1798.135(b).** A consumer may authorize another person solely to opt out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt out request received from a person authorized by		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
		the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General. **Section 3, 1798.135(c).** ***Right to Opt In.*** A business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. **Section 3, 1798.120(c).**		
No discrimination for Exercise of Rights		A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by: (A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties. (C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title. (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data. **Section 3, 1798.125(a).**		A service *provider* shall not discriminate against a road usage charge payer because the road usage charge payer did not give express approval to the service provider to enable sharing of personal information. A service provider may offer a different price, rate, level, or quality of goods or services to the road usage charge payer if that price or difference is directly related to the value provided to the road usage charge payer by the road usage charge payer's personal information. A service provider shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
		A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data. A business that offers any financial incentives shall notify consumers of the financial incentives in the same manner that notice is given that information may be sold. A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature. **Section 3, 1798.125(b).**		
	The right to object shall be explicitly brought to the attention of data subject at the first communication. **A21.4.**			
	For information society services, data subject may exercise right to object by automated means using technical specifications. **A21.5.**			
	Where personal data are processed for scientific or historical research or statistical purposes, the data subject shall have right to object to processing unless the task is carried out for reasons of the public interest. **A21.6.**			

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	In order to comply with the rights to disclose, delete, and not discriminate, a business shall, in a form reasonably accessible, (1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address. (2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable request, but this shall not extend the business's duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's receipt of the verifiable request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable request. (3) For purposes of complying with a verifiable request from the consumer seeking disclosure of information collected: (A) To identify the consumer, associate the information provided by the consumer in the verifiable request to any personal information		

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	previously collected by the business about the consumer. (B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in the definition of "personal information" that most closely describes the personal information collected. (4) For purposes of a request for disclosure of personal information that the business may sell: (A) Identify the consumer and associate the information provided by the consumer in the verifiable request to any personal information previously collected by the business about the consumer. (B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in the definition of "personal information" that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in the definition of "personal information" that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C). (C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in the definition of "personal information" that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the		

WA RUC

European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	enumerated category or categories in the definition of "personal information" that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B). (5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months: (A) A description of a consumer's rights to disclose and not to sell and one or more designated methods for submitting requests. (B) For purposes of disclosure of personal information collected, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories that most closely describe the personal information collected. (C) For purposes of disclosure of personal information that a business may sell, two separate lists: (i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact. (ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
		the preceding 12 months, the business shall disclose that fact. (6) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements for disclosure and nondiscrimination, and how to direct consumers to exercise their rights under those sections. (7) Use any personal information collected from the consumer in connection with the business's verification of the consumer's request solely for the purposes of verification. **Section 3, 1798.130(a).** A business is not obligated to provide the information required for disclosure to the same consumer more than twice in a 12-month period. **Section 3, 1798.130(b).** The categories of personal information required to be disclosed shall follow the definition of personal information. **Section 3, 1798.130(c).**		
Right to decision-making not based solely on automated processing	Data subject has right to not to be subject to decisions based solely on automated processing, including profiling, which produces legal affects but this right shall not apply if the decisions is necessary for entering into or performing a contract between data subject and a data controller or based on the data subject's explicit consent, in which cases controller shall implement suitable safeguards of data subject's rights, freedoms and legitimate interests, at least the right to human intervention to express a point of view or to contest the decision; or is authorized by law. These decisions shall not be based on special categories of personal			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	interest unless consent is given or the public interest is pursued and safeguards are in place to protect the date subject's rights, freedoms and legitimate interests. **A22.1.2.3.4.**			
Restrictions	Member state have the right to enact law restricting the scope of the rights and obligations regarding personal data for certain national interests. **A23.**			
IV. CONTROLLER AND PROCESSOR				
GENERAL OBLIGATIONS				
Responsibility of controller	In context, the controller shall implement appropriate technical and organizational measures to enable and demonstrate that processing is performed in accordance with GDPR, including implementation of data protection policies. Adherence to codes of conduct (A40) or approved certification mechanisms (A42) may demonstrate compliance. **A24.1.2.3.**			
Data protection by design and default	In context, the controller shall implement appropriate technical and organizational measure, including pseudonymization, designed to implement data-protection principles, such as data minimization, and to implement safeguards into processing. **A25.1.**			
	The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data necessary for each specific purpose for processing are processed. **A25.2.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	Approved certification mechanisms (A42) may be used as an element to demonstrate compliance. **A25.3.**			
Joint controllers	Joint controller shall enter into an arrangement for determining their respective responsibilities and duties which duly reflects their roles. Irrespective of an arrangement, the data subject may exercise rights against each of the controllers. **A26.1.2.3.**			
Representatives of controllers or processors not established in EU	Controllers or processors not established in the EU shall designate a representative in writing but shall not apply to pressing that is occasional or by a public authority or body. **A27.**			
Processor	Controllers shall only use processors providing sufficient guarantees to implement appropriate technical and organizational measures that will meet the UE GDPR. **A28.1.**			
	Processor has no authority to engage another processor without authorization by controller. **A28.2.**			
	Processing by processor shall be governed by contract in writing and the contract shall have specific stipulations and can be based on standard contractual clauses. Any processor the processor engages shall be subject to the terms of that contract. **A28.3.4&6.7.8.9.**			
	Adherence to codes of conduct (A40) or approved certification mechanisms (A42) may demonstrate compliance. **A28.5.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	If a processor determines the purposes and means of processing, the processor shall be considered a controller. **A28.10.**			
Processing under authority of controller of processor	Processor or any person acting under authority of controller or processor, who has access to personal data, shall not process those data except on instructions from the controller. **A29.**			
Records of processing activities	Each controller shall maintain in writing a record of certain processing activities under its responsibility which record shall be made available to the supervisory authority upon its request. **A30.1&3.4.**			
	Each processor shall maintain in writing a record of categories of certain processing activities carried out on behalf of the controller which record shall be made available to the supervisory authority upon its request. **A30.2.3.4.**			
	The requirement to maintain a record shall not apply to an organization or enterprise with less than 250 employees unless the processing not occasional and is likely to result in risk of rights and freedoms of data subjects or the processing includes special categories of data relating to racial or ethnic origin, public opinions, religious or philosophical beliefs, trade union membership, and processing of genetic data or biometric data or uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation or personal data relating to criminal convictions or offenses. **A30.5.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Cooperation of supervisory authority	Controller or processor shall cooperate with supervisory authority in the performance of its tasks. **A31.**			
SECURITY OF PERSONAL DATA				
Security of processing	In context, the controller shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of destruction, loss, alteration, unauthorized disclosure of or access to personal data, including the following: • pseudonymization and encryption of personal data; • ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services; • ability to restore availability and access to personal data in a timely manner in event of an incident. **A32.1.2.**			The service provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of destruction, loss, alteration, unauthorized disclosure of or access to personal information, including but not limited to the following: • pseudonymization and encryption of personal information; • ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services; • ability to restore availability and access to personal information in a timely manner in event of an incident. ***Pseudonymization*** means the processing of personal information in a manner that renders the personal information no longer attributable to a specific road usage charge payer without the use of additional information.
	Adherence to codes of conduct (A40) or approved certification mechanisms (A42) may demonstrate compliance. **A32.3.**			
	Controller or processor shall take steps to ensure any natural person acting under their authority does not process personal data except on instructions from the controller unless require by EU or member state law. **A32.4.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Notification of personal data breach	For a personal data breach, the controller shall without undue delay and where feasible, not later than 72 hours after awareness of it, notify the breach to the supervisory authority unless it is unlikely there is risk to rights and freedoms of natural persons. Where notice is not made within 72 hours, it shall contain reasons for the delay. **A33.1.**			For a personal information breach, the service provider shall without undue delay and where feasible, not later than 72 hours after awareness of it, notify the breach to the authorized agency unless it is unlikely there is risk to rights and freedoms of natural persons. Where notice is not made within 72 hours, it shall contain reasons for the delay.
	The notification shall: • describe the nature of the personal data breach, including the categories and approximate number of data subjects and personal data records involved; • communicate the name and contact details of the data protection officer or other contact; • describe the likely consequences; • describe the measures taken to address the personal data breach, its effects and remedial action taken, including measure to mitigate. This information may be provided in phases where this information cannot be provided at the same time. **A33.3.4.**			The notification shall: • describe the nature of the personal information breach, including the categories and approximate number of road usage charge payers and personal information records involved; • communicate the name and contact details of the designated personal information officer of the service provider or other contact; • describe the likely consequences; • describe the measures taken to address the personal information breach, its effects and remedial action taken, including measures to mitigate. This information may be provided in phases where this information cannot be provided at the same time.
	Controller shall document any personal data breaches, including facts, its effects and remedial action taken. **A33.5**			
	Processor shall notify controller of data breach without undue delay after awareness of it. **A33.2.**			
Communication of personal data	Where a personal data breach is likely to result in high risk to rights and freedoms of natural persons, the			Where a personal information breach is likely to result in high risk to rights and freedoms of natural persons, the service

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
breach to data subject	controller shall communicate the breach in clear and plain language to data subject without delay. **A34.1.2.** The communication shall not be required if: • controller has implemented appropriate technical and organizational measures which were applied to the personal data affected by the breach; • controller has taken subsequent measures which ensure high risk to rights and freedoms of data subjects are unlikely to materialize; • it would involve a disproportionate effort and a public communication is made that is equally effective. **A34.3.** If controller makes no communication about a personal data breach, the supervisory authority may require a controller to do so. **A34.4.**			provider shall communicate the breach in clear and plain language to the road usage charge payer without delay. The communication shall not be required if: • service provider has implemented appropriate technical and organizational measures which were applied to the personal information affected by the breach; • service provider has taken subsequent measures which ensure high risk to rights and freedoms of road usage charge payers are unlikely to materialize; • it would involve a disproportionate effort and a public communication is made that is equally effective. If the service provider makes no communication about a personal information breach, the authorized agency may require a service provider to do so.
DATA PROTECTION AND IMPACT ASSESSMENT AND PRIOR CONSULTATION				
Data protection impact assessment	Where a type of processing using new technologies, in context, is likely to result in high risk to rights and freedoms of natural persons, (or there is a change in risk for the processing0, the controller shall, prior to processing and upon the advice of the data protection officer, carry out an assessment of impact of the envisaged processing operations on protection of personal data. **A35.1.2&11.**			
	A data protection assessment shall be required in particular cases:			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• extensive and extensive evaluation of personal aspects of natural persons based on automated processing, including profiling, on which produce legal effects; • processing on a large scale of special categories of data relating to racial or ethnic origin, public opinions, religious or philosophical beliefs, trade union membership, and processing of genetic data or biometric data or uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation or personal data relating to criminal convictions or offenses; • systematic monitoring of a publicly accessible area on a large scale. **A35.3.**			
	Supervisory authority shall establish and make public a list of the kind of processing operation subject to requirement of a data protection assessment. **A35.4.**			
	Monitoring behavior of those on the list with the EU. **A35.6.**			
	The assessment shall contain at least: • a systematic description of the envisaged processing operations, the purposes for processing and the legitimate interest pursued by controller; • an assessment of necessity and proportionality of processing activity in relation to purposes; • an assessment of risks to rights and freedoms of data subjects;			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• measures to address risks, including safeguards, security measures and mechanisms to ensure protection of personal data and demonstrate compliance with EU GDPR. **A35.7.**			
	Compliance with approved codes of conduct (A40) shall be taken into due account in assessing impact of processing operations. **A35.8.**			
	Controller shall seek views of data subjects on the intended processing, where appropriate. **A35.9.**			
	Provision where member state law regulates data protection impact assessment. **A35.10.**			
Prior consultation	Controller shall consult with supervisory authority prior to processing where data protection impact assessment (A35) indicates high risk in the absence of measure to mitigate. **A36.1.** When consulting with supervisory authority, controller shall provide: • respective responsibilities of controller, joint controllers and processors in processing, particularly with a group of undertakings; • purposes and means of intended processing; • measures and safeguards to protect rights and freedoms of data subjects; • contract details of data protection officer; • data protection impact assessment (A35);			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	-other information requested by supervisory authority. **A36.3.**			
	Where supervisory authority has the opinion that intended processing would infringe upon EU GDPR, the authority shall provide written advice to controller or processor and exercise its powers under (A58). **A36.2.**			
	Member states legislative measures on processing. **A36.4.**			
	Authority of member states to require consultation by controllers with supervisory authority. **A36.5.**			
DATA PROTECTION OFFICER				
Designation of data protection officer	Controller and processor shall designate data protection officer in any case where: • processing is carried out by public authority or body; • core activities of controller or processor consist of processing operations which, by their nature, require regular and systematic monitoring of data subjects; • core activities of control or processor consist of processing on a large scale of special categories of data relating to racial or ethnic origin, public opinions, religious or philosophical beliefs, trade union membership, and processing of genetic data or biometric data or uniquely identifying a person, data concerning health or data concerning a natural person's sex life or sexual orientation or personal data relating to criminal convictions or offenses. **A37.1.**			A service provider shall designate a personal information officer to enable contact with road usage charge payers and the authorizing agency for purposes of assuring compliance with this policy. The designated personal information officer may be a staff member of the service provider (or fulfill the tasks on the basis of a service contract) but shall be designated on the basis of professional qualities and expert knowledge of personal information protection under this policy and practices and ability to fulfill tasks.

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	Otherwise, controllers and processors or groups representing categories of them may designate a data protection officer. **A37.4.**			
	A group of undertakings may appoint a single data protection officer provided the person is easily accessible from each establishment. **A37.2.**			
	Where controller or processor is a public authority or body, a single data protection officer may be designated for several such authorities. **A37.3.**			
	The data protection officer may be a staff member of the controller or processor (or fulfill the tasks on the basis of a service contract) but shall be designated on the basis of professional qualities and expert knowledge of data protection law and practices and ability to fulfill tasks (A39). **A37.5.6.**			
	Controller or processor shall publish contact details of the data protection officer. **A37.7.**			
Position of the data protection officer	Controller and processor shall ensure the data protection officer ins involved, properly and in a timely manner, in all issues related to protection of personal data and shall support the data protection officer I performing tasks by providing resources necessary to carry out tasks and access to personal data and processing operations and to maintain expert knowledge. **A38.1.2.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	Controller and processor shall not instruct the data protection officer on performing tasks not shall data protection officer be dismissed or penalized for performing tasks. Data protection officer shall report to highest management level of controller or processor. **A38.1.2.3.**			
	Data subjects may contact data processing officer regarding all issues related to processing of their personal data. **A38.4.**			
	Data protection officer shall be bound by secrecy of confidentiality concerning performance of tasks. **A38.5.**			
	Data protection officer may perform other tasks and duties that do not result in a conflict of interest. **A38.6.**			
Tasks of the data protection officer	At minimum, the data protection office shall have the following tasks: • inform and advise the controller or processor and their employees of their obligations under EU GDPR; • monitor compliance with EU GDPR, other UE or member state data protection provisions and policies of controller or processor related to protection of personal data, including assignment of responsibilities, aware-ness raising and training of staff of processing operations and related audits; • provide advice upon request regarding data protection impact assessment and monitor its performance; • cooperate with supervisory authority;			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• act as contact point for the supervisory authority on issues related to processing and to consult on any other matter. **A39.1.** In performing his tasks, the data protection office shall have due regard to risk associated with processing operations. **A39.2.**			
CODES OF CONDUCT AND CERTIFICATION				
Codes of conduct	EU, member states and the supervisory authorities shall encourage drawing up codes of conduct for proper application of EU GDPR. **A40.1.**			The authorized agency and service providers shall establish, publish and adhere to an organizational usage and privacy policy. The organizational usage and privacy policy shall be available in writing to road usage charge payers, and shall be posted conspicuously on the authorized agency's website and each service provider's website.
	Authorizes associations and other bodies representing categories of controllers and processors to prepare codes of conduct related to application of the EU GDPR. **A40.2.**			The organizational usage and privacy policy shall include: • The authorize purpose for collecting personal information; • The identity and designated tasks for the personal information officer; • Description of the employees and contractors authorized to access and collect personal information and identification of training requirements necessary for the employees and contractors; • Description of how the personal information shall be monitored to ensure compliance with applicable privacy laws and a process for periodic system audits; • Description of reasonable measures that will be used to ensure the accuracy of the personal information and correction of information errors;

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
				• Description of how compliance with security procedures and practices will be implemented and maintained; • Description of how compliance with the rights of road usage charge payers designated by this policy will be maintained; • The period for which the personal information will be stored or retained, by category; • The purpose of, and process for, sharing or disseminating personal information with other persons, whether by those authorized under this policy or by consent of motorists under this policy.
	Codes of conduct may be used by controllers and processors not subject to EU GDPR to provide safeguards for international transfers of personal data. **A40.3.**			
	A code of conduct shall contain mechanisms for carrying out mandatory monitoring of compliance by controllers and processors which undertake to apply it. **A40.4.**			
	Associations and other bodies preparing a code of conduct shall submit a draft code to the supervisory authority which will provide an opinion on compliance with EU GDPR and shall approve the draft code if it finds safeguards prove sufficient. **A40.5.**			
	Supervisory authorities shall register and publish approved draft codes of conduct. **A40.6.**			
	Provisions related to draft codes of conduct for multiple member states			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	and involvement of the EU Commission and Board. **A40.7.8.**			
	EU Commission may decide that approved codes of conduct have general validity within EU and receive appropriate publicity. **A40.9.10.**			
Monitoring of approved codes of conduct	A body monitoring compliance with a code of conduct requires accreditation by a supervisory authority to ensure an appropriate level of expertise relating to the subject matter. **A41. 1.**			
	Accreditation to monitor compliance with a code of conduct requires the following: • demonstrated independence and expertise on the subject-matter; • established procedures to assess eligibility of controller and processors to apply the code, monitor their own compliance and review its operation; • established procedures and structures to handle complaints about infringements of the code of conduct and making those procedures transparent to data subjects and the public; • demonstration to supervisory authority no conflict of interest. **A41.2.**			
	Administration provision related to accreditation. **A41.3.**			
	Accredited body shall take appropriate action in cases of infringement of a code of conduct, including suspension or exclusion. **A41.4.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	Administration provision related to revocation of suspension of accreditation. **A41.5.**			
	This section shall not apply to public authorities and bodies. **A41.5.**			
Certification	Authorized member states to establish data protection certification mechanisms to demonstrate compliance of processing operations with the EU GDPR. **A42.1.**			The authorized agency shall establish certification mechanisms for service providers to demonstrate compliance with the requirements of this policy. Certification bodies shall issue and renew certification on the basis of criteria approved by the authorizing agency. Certification may be withdrawn where requirements for certification are no longer met.
	Accreditation shall be voluntary, last for a maximum or three years, and available via a process that is transparent and provide all information and access to its processing activities which are necessary to conduct certification. Certification may be withdrawn where requirements for certification are no longer met. **A42.3&6.7.**			
	Related to accreditation for processing intended for international purposes. **A42.2.**			
	Certification shall not reduce responsibilities of controller and processor for compliance with EU GDPR. A42.4.			
	Certification shall be issued by certification bodies or a competent supervisory authority on basis of			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	criteria approved according to EU GDPR procedures. A42.5.			
	EU specific administration procedures related to accreditation. **A42.8.**			
Certification bodies	Certification bodies shall issue and renew certification. Certification bodies shall be accredited by: • the competent supervisory authority; • the national accreditation body under EU regulation. Certification bodies shall be accredited for a maximum of five years according to certain criteria set forth in the EU GDPR. **A43.1.2.3.4.**			Independent certification bodies shall be accredited by a competent supervisory authority or a national accreditation body. Certification bodies shall be accredited for a maximum of five years according to certain criteria established by a competent supervisory authority or a national accreditation body.
	EU procedures for accreditation and revocation of accreditation and adoption of technical standards for certification mechanisms. **A43.5.6.7.8.9.**			
V. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS				
General principles for transfers	Personal data undergoing processing and intended for international purposes may be transferred only under certain conditions. **A44.**			
Transfers on the basis of an adequacy decision	Personal data undergoing processing and intended for international purposes may be transferred only under certain conditions. **A45.**			
Transfers subject to appropriate safeguards	Personal data undergoing processing and intended for international purposes may be transferred only under certain conditions. **A46.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Binding corporate rules	Personal data undergoing processing and intended for international purposes may be transferred only under certain conditions. **A47.**			
Transfers or disclosures not authorized by Union law	Personal data undergoing processing and intended for international purposes may be transferred only under certain conditions. **A48.**			
Derogations of specific situations	Personal data undergoing processing and intended for international purposes may be transferred only under certain conditions. **A49.**			
International cooperation for the protection of personal data	Personal data undergoing processing and intended for international purposes may be transferred only under certain conditions. **A50.**			
VI. INDEPENDENT SUPERVISORY AUTHORITIES				
Independent status				
Supervisory authority	Requires each member state to establish at least one supervisory authority to monitor application of the EU GDPR. **A51.**			
Independence	Requires independence for each supervisory authority. **A52.**			
General conditions for members of supervisory authority	Establishes conditions for members of a supervisory authority. **A53.**			
Rules on establishment of supervisory authority	Creates rules for establishment of supervisory authorities. **A54.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
COMPENTANCE, TASKS AND POWERS				
Competence	Requirements for competence for the supervisory authorities. **A55.**			
Competence of lead supervisory authority	Requirements for competence for the lead supervisory authority. **A56.**			
Tasks	Requirements for tasks of the supervisory authorities. **A57.**			
Powers	Requirements for powers for the supervisory authorities. **A58.**			
Activity reports	Each supervisory authority shall draw up an annual report. **A59.**			
VII. COOPERATION AND CONSISTENCY COOPERATION				
COOPERATION				
Cooperation between lead supervisory authority	Specific authorities and responsibilities for UE GDPR administration. **A60.**			
Mutual assistance	Specific authorities and responsibilities for UE GDPR administration. **A61.**			
Joint operations of supervisory authorities	Specific authorities and responsibilities for UE GDPR administration. **A62.**			
CONSISTENCY				
Consistency mechanism	Specific authorities and responsibilities for UE GDPR administration. **A63.**			
Opinions of Board	Specific authorities and responsibilities for UE GDPR administration. **A64.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Dispute resolution by Board	Specific authorities and responsibilities for UE GDPR administration. **A65.**			
Urgency procedure	Specific authorities and responsibilities for UE GDPR administration. **A66.**			
Exchange of information	Specific authorities and responsibilities for UE GDPR administration. **A67.**			
EUROPEAN DATA PROTECTION BOARD				
European data protection board	Specific authorities and responsibilities for UE GDPR administration. **A68.**			
Independence	Specific authorities and responsibilities for UE GDPR administration. **A69.**			
Tasks of Board	Specific authorities and responsibilities for UE GDPR administration. **A70.**			
Reports	Specific authorities and responsibilities for UE GDPR administration. **A71.**			
Procedure	Specific authorities and responsibilities for UE GDPR administration. **A72.**			
Chair	Specific authorities and responsibilities for UE GDPR administration. **A73.**			
Tasks of Chair	Specific authorities and responsibilities for UE GDPR administration. **A74.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Secretariat	Specific authorities and responsibilities for UE GDPR administration. **A75.**			
Confidentiality	Specific authorities and responsibilities for UE GDPR administration. **A76.**			
VIII. REMEDIES, LIABILITY AND PENALTIES				
Right to lodge complaint with supervisory authority	Every data subject has the right to lodge a complaint with a supervisory authority and the supervisory authority shall inform the complainant on the progress and outcome of the complaint and the possibility of judicial remedy. **A77.1.2.**			Every road usage charge payer has the right to lodge a complaint with an authorized agency which shall inform the complainant on the progress and outcome of the complaint and the possibility of judicial remedy.
Right to effective judicial remedy against supervisory authority	Each natural person or legal person has rights to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. **A78.1.**			Each road usage charge payer has rights to an effective judicial remedy against a legally binding decision of an authorized agency concerning them. Each road usage charge payer has a right to an effective judicial remedy where the authorized agency does not handle a complaint or does not inform the road usage charge payer within 3 months on the progress or outcome of complaint lodged.
	Each data subject has a right to an effective judicial remedy where supervisory authority does not handle a complaint or does not inform the data subject within 3 months or progress or outcome of complaint lodged. **A78.2.**			
	Jurisdiction for judicial remedy against supervisory authority. **A78.3.**			
Right to effective judicial remedy	Without prejudiced against any other available administrative or non-			Without prejudice against any other available administrative or non-judicial

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
against controller of processor	judicial remedy, each data subject has the right to an effective judicial remedy where rights are considered to have been infringed from processing personal data in non-compliance. **A79.1.**			remedy, each road usage charge payer has the right to an effective judicial remedy where rights are considered to have been infringed by a service provider in non-compliance with this policy.
	Jurisdiction for judicial remedy against controller or processor. **A79.2.**			
Representation of data subjects	The data subject has the right to mandate that a properly constituted public interest organization present a claim or rights on his/her behalf or a properly constituted public interest may pursue a claim with a mandate if it considers rights have been infringed. **A80.1.2.**			A road usage charge payer has the right to mandate that a properly constituted public interest organization present a claim or rights on his/her behalf.
Suspension of proceedings	A competent court may suspend proceedings it considers duplicative with other proceedings. **A81.**			
Rights to compensation and liability	Imposes rights to compensation for damages suffered and establishes liability for controllers which infringe upon the EU GDPR. Also, establishes sharing of liability among controllers. **A82.1.2.3.4.5.6.**			Road usage charge payers shall have the right to compensation for damages suffered by the actions of service providers which infringe upon rights and responsibilities contained in this policy.
General conditions for imposing administrative fines	Imposes administrative fines for violations of the EU GDPR that are effective, proportionate and dissuasive. When deciding whether to impose fines, due regard should be given to the following: • nature, gravity and duration of the infringement, taking into account the scope or purpose of the processing and the level of damage suffered; • intentional and negligent character of the infringement;		The DOT, in any agreement with a certified service provider, shall provide for penalties if the certified service provider violated these privacy provisions. **ORS 319.915(5).**	Any service provider shall be in violation of this policy for failing to cure any alleged violation within 30 days after notification of alleged noncompliance and therefore liable for civil penalty. Any service provider that intentionally violates this policy shall be liable for a civil penalty of up to $XXXX for each violation but may be adjusted as necessary to ensure the costs incurred by the state are covered.

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	• mitigation that occurred; • degree of controller responsibility; • relevant previous infringements; • degree of cooperation with supervisory authority; • categories of personal data affected; • manner in which the infringement became known to supervisory authority; • measures that have been previously issued against the controller or processor; • adherence to approved codes of conduct or approved certification mechanisms; • any other aggravating or mitigating factor. **A83.1.2.**			
	The administrative fine for a controller infringing upon several provisions of the EU GDPR shall not exceed the fine for the gravest infringement. **A83.3.**			
	Infringements of the following provisions shall be subject to administrative fines of 10,000,000 EUR or, in the case of an undertaking, up to 2 percent of total worldwide annual turnover the preceding financial year, whichever is higher: • obligations of the controller and processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; • obligations of a certification body pursuant to Articles 42 and 43; • obligations of the monitoring body pursuant to Article 41(45). **A83.4.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
	Infringements of the following provisions shall be subject to administrative fines of 20,000,000 EUR or, in the case of an undertaking, up to 4 percent of total worldwide annual turnover the preceding financial year, whichever is higher: • base principles for processing, including conditions for consent pursuant to Articles 5, 6, 7, and 9; • data subjects' rights pursuant to Articles 12 to 22; • transfer of personal data internationally pursuant to Articles 44 to 49; • non-compliance with an order or limitation on processing or suspension of data flows by the supervisory authority. **A83.5.**			
	Non-compliance with an order by a supervisory authority shall be subject to administrative finds up to 20,000,000 EUR or, in the case of an undertaking, up to 4 percent of total worldwide annual turnover the preceding financial year, whichever is higher. **A84.6.**			
	Member states may decide whether and to what extent administrative fines may be imposed on public authorities. **A83.7.**			
	The exercise of supervisory authority powers shall be subject to appropriate procedural safeguards in accordance with EU and member state law, including judicial remedy and due process. Imposes other requirement pertaining to administrative fines by member states. **A83.8.9.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Penalties	Member states have the authority to issue penalties beyond the EU GDPR administrative penalties. **A84.**			
IX. PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS				
Processing and freedom of expression and information	Allows member states to reconcile the right to protection of personal data with the right to freedom of expression and information. **A85.**			
Processing and public access to official documents	Allows member states to reconcile public access to official documents with the right to protection of personal data. **A86.**			
Processing of national identification number	Allows member states to permit processing of a national identification number provided there are appropriate safeguards for the rights and freedoms of data subjects. **A87.**			
Processing in the context of employment	Allows member states to provide more specific rules to protect processing of employees' personal data in employment context with a requirement for safeguards. **A88.**			
Safeguards for archiving in public interest	Requires safeguards for processing for archiving purposes in the public interest, scientific, historical research or statistical purposes. **A89.1.**			
	Allows member states to provide for derogation of rights when such personal data processing rights are likely to render impossible or seriously impair achievement of scientific, historical research or statistical purposes provided there are safeguards. **A89.2.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Obligations of secrecy	Allows member states to adopt specific rules pertaining to the powers of a supervisory authority with regard to an obligation of professional secrecy on the part of controllers and processors and to reconcile right to protection of personal data with the obligation of secrecy. **A90.**			
Existing data protection rules of churches and religious associations	Relates to application of the EU GDPR to churches and religious associations. **A91.**			
X. DELEGATED ACTS AND IMPLEMENTING ACTS				
Exercise of delegation	Delegated acts conferred on European Commission. **A92.**			
Committee procedure	Administration. **A93.**			
XI. FINAL PROVISIONS				
Repeal of Directive 95/46/EC	Specific to EU. **A94.**			
Relationship with Directive 2002/58/EC	Specific to EU. **A95.**			
Relationship with previously concluded Agreements	Specific to EU. **A96.**			
Commission reports	EU administration. **A97.**			
Review of other Union legal acts on data protection	Specific to EU. **A98.**			

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Entry into force and application	Specific to EU. **A99.**			
OTHER PROVISIONS				
Compliance with other laws		California's Consumer Privacy Law does not affect compliance with other federal, state or local laws or civil, criminal, or regulatory inquiries, investigation, or subpoenas or summons issues by federal, state or local authorities or cooperation with law enforcement agencies. Nor does this law affect consumer information that is de-identified or in the aggregate or if every aspect of collecting or selling the personal information takes place wholly outside California. **Section 3, 1798.145(a).**		This policy does not affect compliance with other federal, state or local laws or civil, criminal, or regulatory inquiries, investigation, or subpoenas or summons issues by federal, state or local authorities or cooperation with law enforcement agencies.
- Evidentiary privilege		A consumer's rights to disclosure, no sale and non-discrimination shall not apply where compliance would violate an evidentiary privilege. **Section 3, 1798.145(b).**		
-Health		California's Consumer Privacy Law shall not apply to protected health information. **Section 3, 1798.145(c).**		
-Credit		California's Consumer Privacy Law shall not apply to personal information sold to generate a consumer report and use of that information is limited by the Fair Credit Reporting Act. **Section 3, 1798.145(d).**		
-Financial		California's Consumer Privacy Law shall not apply to personal information collected, processed, sold, or disclosed pursuant to Gramm-Leach-Bliley Act. **Section 3, 1798.145(e).**		
-Driver's privacy		California's Consumer Privacy Law shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act. **Section 3, 1798.145(f).**		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Responding to consumer request		A time period for a business to respond to any verified consumer request may be extended up to 90 additional days where necessary, taking into account the complexity and number of requests. The business shall inform the consumer of any such extension with 45 days of the request, including the reasons for the delay. **Section 3, 1798.145(g)(1).** If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay, of the reasons for not taking action and any rights the consumer may have to repeal. **Section 3, 1798.145(g)(2).** If requests from a consumer are manifestly unfounded or excessive, particularly because of their competitive nature, a business may either charge a reasonable fee or refuse to act and notify the consumer of such. The burden is on the business to demonstrate any such request is manifestly unfounded or excessive. **Section 3, 1798.145(g) (3).**		
Liability		A business that discloses personal information to a service provider shall not be liable if the service provider receiving personal information from the business uses it in violation of restrictions set forth in the California Consumer Privacy Law if the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. **Section 3, 1798.145(h).**		
Construing Consumer Privacy Law		California's Consumer Privacy Law shall not be construed to a business to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information. **Section 3, 1798.145(j).**		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Consumer Privacy Law's relationship to other rights		The rights afforded to consumers and the obligation imposed on the business by the California Consumer Privacy Law shall not adversely affect the rights and freedoms of other consumers. ***Section 3, 1798.145(i).***		
Civil action for security violations		Any consumer whose nonencrypted or nonredacted personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty of to implement and maintain reasonable security practices may institute a civil action to recover damages (not less than $100 or greater than $750 per incident or actual damages, based on circumstances, whichever is greater, injunctive or declaratory relief, or any other relief the court deems proper. **Section 3, 1798.150(a).** Requirements to bring civil action for security violations. **Section 3, 1798.150(b).** Relationship of civil action for security violations to other laws and other duties or obligations. **Section 3, 1798.150(c).**		Any road usage charge payer whose personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty of to implement and maintain reasonable security practices may institute a civil action to recover damages not less than $XXX or greater than $XXX per incident or actual damages, based on circumstances, whichever is greater, injunctive or declaratory relief, or any other relief the court deems proper.
Civil action brought by Attorney General		Any business or third party shall be in violation of the California Consumer Privacy Law for failing to cure any alleged violation within 30 days after notification of alleged noncompliance and therefore liable for civil penalty in an action brought by the Attorney General. **Section 3, 1798.155(a).** Any person, business or service provider that intentionally violated the California Consumer Privacy Law shall be liable for a civil penalty of up to $7,500 for each violation but may be adjusted as necessary to ensure the costs incurred by the state and Attorney General are covered. **Section 3, 1798.155(b)(d).**		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
		Allocation of civil penalty. **Section 3, 1798.155(c).**		
Consumer Privacy Fund		The Consumer Privacy Fund is created to offset any cost incurred by Attorney General in carrying out duties under the California Consumer Privacy Law. **Section 3, 1798.160**		
Application of this law		The California Consumer Privacy Law applies to collection and sale of all personal information collected by a business from consumers and is not limited to information collected electronically over the Internet. **Section 3, 1798.175.**		
Preemption of local law		The California Consumer Privacy Law is a matter of statewide concern and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, municipality, or other local agency. **Section 3, 1798.180.**		
Regulations		The Attorney General shall solicit broad public participation to adopt regulations on or before January 1, 2010. **Section 3, 1798.185.**		The authorized agency shall solicit broad public participation to adopt regulations on or before the operative date for this policy.
Attempts to avoid the reach of this law		If a series of steps or transactions were component parts of a single transaction intended to avoid the reach of the California Consumer Privacy Law, a court shall regard the intermediate steps or transactions. **Section 3, 1798.190.**		If a series of steps or transactions were component parts of a single transaction intended to avoid the reach of this policy, a court shall regard the intermediate steps or transactions.
Inapplicability of waiver		Any provision in a contract that purports to waive or limit consumer rights under the California Consumer Privacy Law shall be void and unenforceable. **Section 3, 1798.192.**		Any provision in a contract that purports to waive or limit road usage charge rights under this policy shall be void and unenforceable.
Construction of this law		The California Consumer Privacy Law shall be liberally construed to effectuate its purposes. **Section 3, 1798.194.**		

WA RUC

	European Union General Data Protection Regulation	California Consumer Privacy Act of 2018 (Title 1.81.5)	Oregon Road Usage Charge Program (ORe*GO*) Privacy Protection Provisions	Model RUC Privacy Policy for US States
Preemption by federal law or California Constitution		The California Consumer Privacy Law is intended to supplement federal and state law but shall not apply if such application is preempted by, or in conflict with, federal law or the California Constitution. **Section 3, 1798.196.**		
Operative date		The California Consumer Privacy Law becomes operative January 1, 2020. **Section 3, 1798.198.**		