APPENDICES TO THE DATA PROCESSING AGREEMENT

THIS DOCUMENT CONSTITUTES THE FOLLOWING APPENDICES:

APPENDIX A – INFORMATION REGARDING THE PROCESSING

APPENDIX B - CONDITIONS FOR THE DATA PROCESSOR'S USE OF SUB-PROCESSORS

APPENDIX C - INSTRUCTIONS REGARDING THE PROCESSING OF PERSONAL DATA

APPENDIX D - CHANGES TO THE STANDARD TEXT OF THE DATA PROCESSING AGREEMENT AND SUSEQUENT CHANGES AFTER ENTERING INTO THE AGREEMENT

A. INFORMATION ABOUT THE PROCESSING

A.1 **The Main Agreement and the purpose of the processing of personal data**

The Data Processor's processing of personal data on behalf of the Data Controller pertains to the delivery of services as described in the Main Agreement.

The Main Agreement is the following agreement(s) entered into between the Parties:

Agreement on Non-domestic toll collection (SSA-L), entered into [date XX.XX.XXXX].

The purpose of the processing is as follows:

- *Collection of tolls from non-domestic vehicles, as described in Appendix 1 with annexes to the Main Agreement.*

A.2 **The Data Processor's processing of personal data on behalf of the Data Controller**

The Data Processor's processing of personal data on behalf of the Data Controller concerns (nature of the processing):

- *Collection of information (including pictures) from each toll company about vehicle owners' passing of toll booths.*
- *Collection and storage of owner information from various vehicle registers based on registration numbers collected from the regional toll companies. Look up in Appendix 1 to the Main Agreement for a more detailed description.*

A.3 **Types of personal data**

The processing concerns the following types of personal data concerning the data subjects (several options are possible):

☐	*Special categories of personal data in accordance with Article 9 (1) of GDPR.*
☒	*Other information subject to a special need for protection:* *It may be necessary to process national identity number or financial details in certain cases.*
☒	*Other personal data:* *Name, vehicle registration number, photos showing time of toll booth passage, etc.*

A.4 **Categories of data subjects**

The processing concerns the following categories of data subjects:

- *Owners and users of foreign vehicles passing Norwegian toll booths.*

A.5 **Duration of processing**

Processing of personal data by the Data Processor under the Main Agreement may commence when the Data Processing Agreement has entered into force. The processing has the following duration (select one option):

☒	The processing is not limited in time and lasts until the expiry of the Main Agreement.
☐	The processing is limited in time and applies until *<state date or criterion for termination, such as the conclusion of a project. Note that the processing may not normally be concluded before the Main Agreement expires >.*

On expiry (of the Main Agreement or the processing), personal data must be returned and erased in accordance with section 12 of the Data Processing Agreement and the instructions in Appendix C.

B. CONDITIONS FOR THE DATA PROCESSOR'S USE OF AND CHANGES IN ANY SUBPROCESSORS

B.1   **The Data Controller's approval of the use of Subprocessors**

When entering into the Data Processing Agreement, the Data Controller approves the use of the Subprocessors listed in section B.2. Note that parent and sister companies and subsidiaries of the Data Processor are also considered to be Subprocessors if they contribute to the delivery of services and process personal data.

The following is agreed concerning changes in the use of Subprocessors:

☒	The Data Processor may use a Subprocessor from the same Group (parent or sister company or subsidiary) that is established in a country within the EEA. The Data Processor must inform the Data Controller in advance of the use of any such Subprocessor. (This option can be combined with one of the other options.)
☒	The Data Processor may make changes to the use of Subprocessors provided that the Data Controller is notified and is given the opportunity to object to the changes. Any such notification must be received by the Data Controller no later than one month before the change enters into force, unless otherwise agreed in writing between the Parties. Changes that entail the transfer of personal data to countries outside the EEA (third countries) still require written approval pursuant to section 10 of the Data Processing Agreement. If the Data Controller opposes the change, the Data Processor must be notified as soon as possible. The Data Controller may only object to the change on reasonable and justifiable grounds.
☐	The Data Processor may only make changes to the use of Subprocessors with the specific prior written approval of the Data Controller. The Subprocessor may not process personal data under the Main Agreement before such approval has been granted. Approval shall not be unreasonably withheld.

Note: If the Data Processor uses subcontractors (third parties) that deliver standardised third-party services (typically cloud services), and that fulfil the terms of section 9.7 of the Data Processing Agreement, so that the third party's standard data processing agreement is applied directly to the Data Controller, any subcontractor replacement by the third party will adhere to the provisions of the third party's data processing agreement.

B.2 **Approved Subprocessors**

The Data Controller has approved the following Subprocessors:

Name	Reg. no.	Address	Description of processing	Processing location	Contact details	Special categories of personal data
[Name]	[Reg.no.]	[Address]	[Overall description of the processing to be performed by the Subprocessor]	[State the country where the data is stored, from where access to data is gained, or in which the data is processed by other means]	[Contact details]	[Specify whether special categories of personal data are processed]
[Name]	[Reg.no.]	[Address]	[Overall description of the processing to be performed by the Subprocessor]	[State the country where the data is stored, from where access to data is gained, or in which the data is processed by other means]	[Contact details]	
[Name]	[Reg.no.]	[Address]	[Overall description of the processing to be performed by the Subprocessor]	[State the country where the data is stored, from where access to data is gained, or in which the data is processed by other means]	[Contact details]	
[Name]	[Reg.no.]	[Address]	[Overall description of the processing to be performed by the Subprocessor]	[State the country where the data is stored, from where access to data is gained, or in which the data is processed by other means]	[Contact details]	

The Data Processor may not use the individual Subprocessor for any other processing than as agreed or allow another Subprocessor to perform the processing described in cases other than as described in Appendix B, section B.1 concerning the replacement of a Subprocessor.

C. INSTRUCTIONS CONCERNING THE PROCESSING OF PERSONAL DATA

C.1 **Scope and purpose of processing**

The personal data may only be processed within the scope and for the purpose described in the

- Main Agreement
- Data Processing Agreement with appendices

The Data Processor does not have the right to use the personal data other than to the extent necessary to fulfil its obligations under the Data Processing Agreement and may not process this data for the Data Processor's own purposes.

C.2 **Security of processing**

C.2.1 *Specification of security level*

A specific risk assessment based on an assessment of the scope of the personal data that is processed, the type of information and the nature of the processing, determines that the processing (select one option):

☐ Requires a high security level. Reason:

<Refer to the risk assessment made and write the reason>

☒ Does not require a high security level. Reason:

The Customer do not transmit particularly sensitive personal data to the Supplier. However, it is important that photos of toll passes do not go astray. The Customer assumes that the Supplier conducts its own risk assessment and handles the personal data particularly carefully if the degree of sensitivity so indicates.

C.2.2   *Information security management system*

The Data Processor must have an appropriate system for managing information security. The Data Processor must establish and manage adequate security measures to protect information security concerning the processing of personal data, including (several options are possible):

☒	Security requirements as described in the Main Agreement: *SSA-L chapter 6.*
☐	Security requirements as described below:

C.3   **Documentation**

The Data Processor shall document the procedures and measures taken to fulfil the requirements arising from the Applicable Privacy Policy and the Data Processing Agreement, including the information security requirements. This documentation must be stored and updated for the duration of the Data Processing Agreement and shall be made available to the Data Controller or supervisory authorities on request.

C.4   **Transfer of personal data - Location for processing and access**

Without the prior written approval of the Data Controller, processing of the personal data covered by the agreement may not take place at or with access from other locations than those specified in Appendix B.2. By location is meant:

- Place from where it is possible to access the personal data (access)
- Place where the personal data is handled (processed)
- Place where the personal data is stored

This limitation does not apply to parent and sister companies and subsidiaries of the Data Processor that are established within the EEA. At the request of the Data Controller, the Data Processor must, however, be able to document where the personal data is processed at any time.

C.5 **Auditing and supervision procedures**

In order to monitor compliance with the Applicable Privacy Policy and the Data Processing Agreement, the following has been agreed (several options are possible):

☒	The Data Controller has the right to conduct audits at the Data Processor's place of business in order to verify the Data Processor's compliance with its obligations under this Data Processing Agreement or the Applicable Privacy Policy. Such audits shall: • Be subject to reasonable advance notice and shall be performed no more than once per year, unless a security breach at the Data Processor or other special circumstances justify more frequent audits • Take place during normal working hours and without unnecessary disruption of the Data Processor's work-related activities • Be performed by employees of the Data Controller or by third parties who are approved by the Parties and are subject to an obligation of confidentiality. The Data Processor shall make available the necessary resources reasonably required in order to perform the audit. The Data Controller shall cover the costs of any third parties used to conduct the audit. Each Party will cover their own costs pertaining to the performance of the audit. If the audit reveals significant breaches of the obligations under the Applicable Privacy Policy or the Data Processing Agreement, the Data Processor must nonetheless cover the Data Controller's reasonable costs ensuing from audit.

☐	The Data Processor will engage an external auditor to verify that security measures have been put in place and are working as intended. This audit must:
	   i. take place once a year,
	   ii. be performed in accordance with recognised verification standards, such as ISAE 3402, and
	   iii. be performed by an independent third party with sufficient knowledge and experience.
	
	The reports must be submitted to the Data Controller on request.
	
	The Data Processor must also provide the information and assistance necessary for the Data Controller to be able to comply with its obligations under the Applicable Privacy Policy.

☐	Third-party audits may be submitted, where standardised third-party services are provided by a Subprocessor, as long as the audit took place in accordance with generally recognised principles and by a certified auditor.

C.6 **Erasure and return of personal data upon the expiry of the agreement**

The Parties have agreed on the following regarding erasure/return of personal data (select one option):

☐	All personal data processed under this Data Processing Agreement must be erased without undue delay and no later than within 90 calendar days of the expiry of the Main Agreement. The same applies to any other relevant information managed on behalf of the Data Controller.
☐	All personal data processed under this Data Processing Agreement, and any other relevant information managed on behalf of the Data Controller, must be returned upon the expiry of the Main Agreement. Within 30 calendar days after return has taken place, the Data Processor is required to erase all personal data and other relevant information managed on behalf of the Data Controller. Return must take place as follows: *<Specify how and which format is to be used for the return of data>*
☒	All personal data processed under this Data Processing Agreement must be erased without undue delay and no later than within 90 calendar days of the expiry of the Main Agreement. The same applies to any other relevant information managed on behalf of the Data Controller. "the expiry of the Mail Agreement" = when the Supplier has closed all the cases that the Customer has submitted, cf. SSA-L Appendix 5.

C.7 Sector-specific provisions concerning the processing of personal data
None.

Version 01.2020

C.8 **Contact details**

For any enquiries pursuant to this Agreement, such as notification of breach of personal data security or a change in the use of Subprocessors, the following channels must be used:

At the Data Controller	**At the Supplier**
<u>Security breach:</u>	<u>Security breach:</u>
Phone: *[Complete]*	Phone: *[Complete]*
Email *[Complete]*	Email *[Complete]*
<u>Other enquiries:</u>	<u>Other enquiries:</u>
Name: *[Complete]*	Name: *[Complete]*
Position: *[Complete]*	Position: *[Complete]*
Phone: *[Complete]*	Phone: *[Complete]*
Email *[Complete]*	Email *[Complete]*

Version 01.2020

D. CHANGES TO THE STANDARD TEXT OF THE DATA PROCESSING AGREEMENT AND CHANGES AFTER THE ESTABLISHMENT OF THE AGREEMENT