Highways England Company Limited

Scope

Data Protection

Annex 8

LIST OF CONTENTS

1 DATA PROTECTION

1.1 Data Protection

1.1.1. For the purposes of this contract and the Data Protection Legislation:

- for the purposes of this section only the *Client* is the Controller, and
- the *Consultant* is the Processor and
- this section and Schedule [A] (data protection) together constitute a data processing agreement where required by the Data Protection Legislation.

1.1.2. The *Consultant* processes the Data in accordance with the Data Protection Legislation and only to the extent necessary for the purpose of Providing the Service.

1.1.3. The *Consultant* complies with the requirements of Procurement Policy Note 02/18 entitled 'Changes to Data Protection Legislation & General Data Protection Regulation' ('**PPN 02/18'**) or any later revision (see link at **Annex 02**) and any related supplementary Procurement Policy Notes in Providing the Service.

1.1.4. The *Consultant* does not knowingly do anything or permit anything to be done which might lead to a breach of the Data Protection Legislation by either Party.

1.1.5. The *Consultant* obtains and maintains until Completion all registrations and notifications that it is obliged to obtain and maintain pursuant to the Data Protection Legislation (see link in **Annex 02**) in respect of Providing the Service.

1.1.6. The *Consultant* only processes Data to the extent it relates to;

- the types of Data,
- the categories of Data Subject and
- the nature and purpose

Set out in Schedule [A] (data protection) and only for the duration specified in Schedule [A] (data protection).

1.1.7. Without prejudice to 1.1.2 the *Consultant* processes the Data only in accordance with the instructions of the *Service* unless the *Consultant* is required to process Data for other reasons under the laws of the European Union (or a member state of the EEA) to which the *Consultant* is subject. If the *Consultant* is required to process the Data for these other reasons, it informs the *Client* before carrying out the processing, unless prohibited by relevant law.

1.1.8. The *Consultant* immediately informs the *Client* if it believes that an instruction infringes the Data Protection Legislation or any other applicable law.

1.1.9. The *Consultant* has in place and maintains in accordance with then good industry practice for as long as it holds any Data taking into account the state of the art, the costs of implementing, the harm that might result from a Data Loss Event and the nature, scope, context and purposes of processing

- appropriate technical and organisational measures to protect the Data against accidental, unauthorised or unlawful processing, destruction, loss, damage, alteration or disclosure and
- adequate security programmes and procedures to ensure that unauthorised persons do not have access to the Data or to any equipment used to process the Data.

in each case to ensure that the *Consultant's* processing is in accordance with the Data Protection Legislation and protects the rights of Data Subjects.

1.1.10. The *Consultant* submits details of its Protective Measures to the *Client* for acceptance. A reason for not accepting them is that they are not appropriate to protect against a Data Loss Event. Acceptance (or a failure to reject) by the *Client* does not amount to approval by the Controller of the adequacy of the Protective Measure.

1.1.11. The *Consultant* ensures that all persons authorised to process Data are bound by obligations equivalent to those set out in clause Z5 (Confidentiality) and this section and are aware of the *Consultant's* obligations under the contract and the Data Protection Legislation.

1.1.12. The *Consultant* ensures access to the Data is limited to those persons who need access in order for the *Consultant* to Provide the Service and (in each case) to such parts of the Data as are strictly necessary for performance of that person's duties.

1.1.13. Not Used.

1.1.14. On request, the *Consultant*, takes all necessary actions and provides the *Client* with all reasonable assistance necessary for the *Client* to comply with a Data Subject Request, including;

- the provision of access to, and information relating to, Data,
- the rectification of inaccurate Data,
- the permanent erasure of Data
- the restriction of processing of Data,
- the provision of a copy of Data in machine readable format, and
- the transfer of Data to a third party.

1.1.15. The *Consultant* immediately notifies the *Client* if it receives

- a Data Subject Request (or purported Data Subject Request);
- a complaint or request relating to the *Client's* obligations under the Data Protection Legislation, or
- a request from any Supervisory Authority for assistance or information, unless provided by relevant law.

1.1.16. The *Consultant* assists and co-operates with the *Client* in relation to any complaint or request received, including

- providing full details of the complaint or request
- complying with the request within the time limits set out in the Data Protection Legislation and in accordance with the instructions of the *Client* and
- promptly providing the *Client* with any Personal Data and any other information requested by it to enable it to respond to the request.

1.1.17. The *Consultant* does not process the Data outside the EEA (other than in the United Kingdom) without the agreement of the *Client.* Where the *Client* agrees, the *Consultant*

- Provides evidence (acceptable to the *Client*) of appropriate safeguards as required by the Data Protection Legislation and
- Complies with the instructions of the *Client.*

1.1.18. The *Consultant* complies with the requirements of the *Client* in relation to the storage, dispatch and disposal of Data in any form or medium. Any requirement for the *Consultant* to destroy or delete copies of the Data is subject to any law of the European Union (or a member state of the EEA) to which the *Consultant* is subject that requires Data to be retained.

1.1.19. The *Consultant* notifies the *Client* within 24 hours of becoming aware of a Security Incident or any other breach of this section. The notification includes, as far as possible.

- a description of the nature of the Security Incident, including the categories and approximate number of Data Subjects concerned.
- the likely consequences of the breach and
- the Protective Measures taken, or to be taken, to address the breach, including measures taken to mitigate any possible adverse effects [including those outlined in PPN 02/18].

1.1.20. In the event of a Security Incident, the *Consultant* provides the *Client* with full co-operation and assistance in dealing with the Security Incident, in

particular in notifying individuals affected by the Security Incident or a Supervisory Authority as required by the Data Protection Legislation.

1.1.21. On request (but not more than once in any 12-month period) the *Consultant* provides to the *Client* all necessary information to demonstrate the *Consultant* compliance with this section.

1.1.22. The *Consultant* promptly provides assistance and information requested by any Supervisory Authority or required by the *Client* in order for the *Client* to ensure compliance with its obligations under the Data Protection Legislation, including in relation to

- security of processing,
- preparation of any necessary Data Protection Impact Assessments and
- undertaking any necessary data protection consultations.

1.1.23. The *Consultant* maintains electronic records of all processing activities carried out on behalf of the *Client*, including:

- the information described in 1.1.6 of this annex.
- The different types of processing being carried out (if applicable),
- any transfers of Data outside the EEA or the United Kingdom, identifying the relevant country or international organisations and any documentation required to demonstrate suitable safeguards and
- a description of the technical and organisation security measures referred to in 1.1.9 of this annex.

The *Consultant* makes these records available to the *Client* promptly on request.

1.1.24. The *Consultant* does not engage any Sub-Processor without the prior consent of the *Client.*

1.1.25. Before allowing any Sub-Processor to process any Personal Data related to this agreement, the Processor must:

- notify the Controller in writing of the intended Sub-Processor and processing;
- obtain the written consent of the Controller;
- enter into a written agreement with the Sub-Processor which give effect to the terms set out in this clause such that they apply to the Sub-Processor; and
- provide the Controller with such information regarding the Sub-Processor as the Controller may reasonably require.

1.1.26. The Processor shall remain fully liable for all acts or omissions of any of its Sub-Processors.

1.1.27. The Controller may, at any time on not less than 30 working days' notice, revise this clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this agreement).

1.1.28. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 working days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.1.29. Each Party shall designate its own Data Protection Officer if required by the Data Protection Legislation.

1.1.30. Not used.

1.1.31. If it is or becomes a requirement that, under the Data Protection Legislation or other applicable laws, this section must be governed by the laws of a member state of the European Union, and the *law of the contract* does not or ceases to satisfy this requirement, this section is governed by and construed in accordance with the laws of Ireland.

1.1.32. A failure to comply with this section is treated as a substantial failure by the *Consultant* to comply with its obligations.

2 DATA PROTECTION (SCHEDULE [A])

2.1 Schedule [A] – Processing, Personal Data and Data Subjects

This Schedule shall be completed by the *Client,* who may take account of the view of the *Consultants,* however the final decision as to the content of this Schedule shall be with the *Client* at its absolute discretion

1. The contact details of the *Client's* Data Protection Officer are Graham Woodhouse (dataprotectionadvice@highwaysengland.co.uk).

2. The contact details of the *Consultant* Data Protection Officer or nominated lead are per Contract Data part 2.

3. The *Consultant* shall comply with any further written instructions with respect to processing by the *Client*.

Any such further instructions shall be incorporated into this table.

Description	Details
Identity of the *Client* and *Consultant*	The Parties acknowledge that for the purposes of the Data Protection Legislation, the *Client* is the Controller and the *Consultant* is the Processor in accordance with clause 2.
Subject matter of the processing	The *Consultant* will be responsible for gathering and processing information on the Supply Chain and wider Supplier Markets to inform the *Client* and deliver reports as part of this service.
Duration of the processing	The *Consultant* will process information throughout the duration of the contract, including throughout any extension period as confirmed by the *Client.*
Nature and purposes of the processing	The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The *Consultant* will be gathering data from primary and secondary sources, including expert interviews and, carrying out analysis to produce detailed reports for the *Client.*
Type of Personal Data	Types of Personal Data would include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc. The *Consultant* is responsible for the secure handling and processing of all Personal Data in relation to this Contract. This is likely to include names of the *Client's* employees and Supply Chain contacts that are involved, at any stage, in the delivery of this service.
Categories of Data Subject	May include: Staff (including volunteers, agents, and temporary workers), suppliers, members of the public etc.

Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The *Consultant* should arrange to securely transfer any data requested by the Client within 4 weeks from the end of contract and subsequently arrange for the secure destruction of the remaining data from the Consultants systems, at the discretion of the Contract Manager and *Client.*

3 NOT USED