National Highways Limited

Scheme Delivery Framework (SDF)

Framework Information

Appendix 14

Data Protection

CONTENTS AMENDMENT SHEET

Issue No.	Revision No.	Amendments	Initials	Date
0	0	Contract Issue	AJP	Sept 21

LIST OF CONTENTS

1 DATA PROTECTION 4

1.1 Data Protection 4

2 DATA PROTECTION (SCHEDULE A) 9

2.1 Schedule A – Processing, Personal Data and Data Subjects 9

1 DATA PROTECTION

1.1 Data Protection

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

- for the purposes of this Appendix only the *Client* is the Data Controller,
- the *Supplier* is the Processor and
- this Appendix and schedule A (data protection) together constitute a data processing agreement where required by the Data Protection Legislation.

1.1.2. The *Supplier* processes the Data in accordance with the Data Protection Legislation and only to the extent necessary for the purpose of providing the service or providing the works.

1.1.3. The *Supplier* 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.

1.1.4. The *Supplier* obtains and maintains until the *end date* all registrations and notifications that it is obliged to obtain and maintain pursuant to the "Data Protection Legislation" in **Appendix 2** in respect of providing the service or providing the works.

1.1.5. The *Supplier* only processes Data to the extent it relates to

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

as set out in schedule A (data protection) and only for the duration specified in schedule A (data protection).

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

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

1.1.8. The *Supplier*

- implements and maintains Protective Measures which take into account the nature, scope, context and purpose of processing the Data and
- implements 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.

The *Supplier* ensures its processing is in accordance with the Data Protection Legislation and protects the rights of Data Subjects.

1.1.9. The *Supplier* 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 Security Incident. Acceptance (or a failure to reject) by the *Client* does not amount to acceptance by the *Client* of the adequacy of the Protective Measures.

1.1.10. The *Supplier* ensures that all persons authorised to process Data are bound by obligations equivalent to those set out in the Framework Agreement ("Confidentiality") and this Appendix and are aware of the *Supplier's* obligations under the contract and the Data Protection Legislation.

1.1.11. The *Supplier* ensures access to the Data is limited to those persons who need access in order for the *Supplier* to provide the service or provide the works and (in each case) to such parts of the Data as are strictly necessary for performance of that person's duties.

1.1.12. Not used

1.1.13. On request, the *Supplier*, takes all necessary actions and provides the *Client* with all reasonable assistance necessary for the *Client* to comply with a Data Subject Access Request.

1.1.14. The *Supplier* immediately notifies the *Client* if it receives

- a Data Subject Access Request (or purported Data Subject Access 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.

1.1.15. The *Supplier* assists and co-operates with the *Client* in relation to any complaint or Data Subject Request received pursuant to paragraph 1.1.14, including

- providing full details of the complaint or Data Subject Access Request,

- complying with the Data Subject 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* through the *Client* with any Personal Data and any other information requested to enable it to respond to the Data Subject Request within the time limits set out in the Data Protection Legislation.

1.1.16. The *Supplier* 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 *Supplier*

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

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

1.1.18. The *Supplier* notifies the *Client* as soon as they become 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.

1.1.19. In the event of a Security Incident, the *Supplier* 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 and in accordance with the instructions of the *Client*.

1.1.20. On request the *Supplier* provides to the *Client* all necessary information to demonstrate the *Supplier* compliance with this Appendix.

1.1.21. The *Supplier* promptly provides all 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 of Supervisory Authorities.

1.1.22. The *Supplier* maintains electronic records of all processing activities carried out on behalf of the *Client*, including

- the information described in paragraph 1.1.5 of this Appendix,
- the different types of processing of Data 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 paragraph 1.1.9 of this Appendix.

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

1.1.23. Before allowing any Sub-Processor to process any Personal Data related to the contract, the *Supplier*

- notifies the *Client* in writing of the intended Sub-Processor and processing,
- obtains the written agreement of the *Client*,
- enters into a written agreement with the Sub-Processor which give effect to the terms set out in the contract such that they apply to the Sub-Processor and
- provide the *Client* with such information regarding the Sub-Processor as the *Client* may reasonably require.

1.1.24. The *Client* may, at any time revise this Appendix by replacing it with any applicable controller to processor standard provisions or similar terms forming part of an applicable certification scheme.

1.1.25. The Parties agree to take account of any guidance issued by the Information Commissioner's Office.

1.1.26. Each Party designates its own Data Protection Officer if required by the Data Protection Legislation.

1.1.27. Not used

1.1.28. A failure to comply with this Appendix is treated as a substantial failure by the *Supplier* 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 *Supplier,* 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 *Supplier* Data Protection Officer or nominated lead are per Contract Data part 2.

3. The *Supplier* complies with any further written instructions with respect to processing by the *Client*.

Any such further instructions are to be incorporated into this table.

Column A Description	Column B Framework Information (generic information)	Column C Work Order (specific information)
Identity of the *Client* and *Supplier*	The Parties acknowledge that for the purposes of the Data Protection Legislation, the *Client* is the Controller and the *Supplier* is the Processor in accordance with clause 2, unless otherwise stated in Column C.	As stated in the Framework Information.
Subject matter of the processing	The processing is needed in order to ensure that the *Supplier* can effectively perform and discharge their obligations in relation to any contract instructed pursuant to this Framework Agreement.	As stated in the Framework Information.
Duration of the processing	The Term of the Framework Contract.	As stated in the Framework Information.
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 purpose of the processing might include: employment processing, relevant statutory obligations, assessment, verification, contract compliance, monitoring and/or reporting.	As stated in the Framework Information.

Type of Personal Data	Name Company Address Work Telephone number Work Email address and any further type of Personal Data stated in Column C.	Client Name Company Address Work Telephone number Work Email address and as stated in the Framework Information.
Categories of Data Subject	Staff (including volunteers, agents, and temporary workers), Other Suppliers Third parties such as insurers and any further categories of Data Subject stated in Column C.	As stated in the Framework Information.
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 data will be preserved for twelve years from Scheme completion. This is to allow the *Client* to follow up on any queries.	As stated in the Framework Information.