

Highways England Company Limited

Area 9

Asset Delivery (AD)

Scope

Annex 29

Data Protection

CONTENTS AMENDMENT SHEET

Amend No	Revision No.	Amendments	Initials	Date
0	0	Tender Issue	AP	30/06/2021

LIST OF CONTENTS

1	DATA PROTECTION	4
1.1	Data Protection	4

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 section only the *Client* is the Controller, and
 - the *Contractor* is the Processor and
 - this annex constitutes a data processing agreement where required by the Data Protection Legislation.
- 1.1.2. The *Contractor* 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 *Contractor* 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 *Contractor* obtains and maintains until end of the *service period* all registrations and notifications that it is obliged to obtain and maintain pursuant to the Data Protection Legislation (see link in Annex 3) in respect of Providing the Service.
- 1.1.5. The *Contractor* only processes Data to the extent it relates to;
- the types of Data,
 - the categories of Data Subject and
 - the nature and purpose
- 1.1.6. Without prejudice to 1.1.2 the *Contractor* processes the Data only in accordance with the instructions of the *Service Manager* unless the *Contractor* 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 *Contractor* is subject. If the *Contractor* is required to process the Data for these other reasons, it informs the *Service Manager* before carrying out the processing, unless prohibited by relevant law.
- 1.1.7. The *Contractor* immediately informs the *Service Manager* if it believes that an instruction infringes the Data Protection Legislation or any other applicable law.
- 1.1.8. The *Contractor*
- implements and maintains Protective Measure 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 *Contractor* ensures its processing is in accordance with the Data Protection Legislation and protects the rights of Data Subjects.

- 1.1.9. The *Contractor* submits details of its Protective Measures to the *Service Manager* 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 Measure.
- 1.1.10. The *Contractor* ensures that all persons authorised to process Data are bound by obligations equivalent to those set out in clause Z7 (Confidentiality) and this annex and are aware of the *Contractor's* obligations under the contract and the Data Protection Legislation.
- 1.1.11. The *Contractor* ensures access to the Data is limited to those persons who need access in order for the *Contractor* 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.
- 1.1.12. Where the *Contractor* obtains or collects Personal Data on behalf of the *Client*, the *Contractor*
- provides to Data Subjects a data protection notice in a form accepted by the *Service Manager* informing the Data Subject of the identity of the *Client*, the identify of any data protection representative it may have appointed, the purpose or purposes for which their Personal Data will be processed and any other information which is necessary having regard to the specific circumstances in which the Personal Data is, or is to be, processed to enable processing in respect of the Data Subject to be fair and comply with the Data Protection Legislation; and
 - where applicable, obtains all necessary consents for the processing of Data.
- 1.1.13. On request, the *Contractor*, takes all necessary actions and provides the *Service Manager* with all reasonable assistance necessary for the *Client* to comply with a Data Subject Access Request.
- 1.1.14. The *Contractor* immediately notifies the *Service Manager* 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 *Contractor* assists and co-operates with the *Service Manager* in relation to any complaint or Data Subject Access 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 Access Request within the time limits set out in the Data Protection Legislation and in accordance with the instructions of the *Service Manager*, and
 - promptly providing the *Client* through the *Service Manager* with any Personal Data and any other information requested to enable it to respond to the Data Subject Access Request within the time limits set out in the Data Protection Legislation.
- 1.1.16. The *Contractor* does not process the Data outside the EEA (other than in the United Kingdom) without the agreement of the *Service Manager*. Where the *Client* agrees, the *Contractor*
- provides evidence (acceptable to the *Service Manager*) of appropriate safeguards as required by the Data Protection Legislation and
 - complies with the instructions of the *Service Manager*.
- 1.1.17. The *Contractor* complies with the requirements of the *Client* and the *Service Manager* in relation to the storage, dispatch and disposal of Data in any form or medium. Any requirement for the *Contractor* 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 *Contractor* is subject that requires Data to be retained.
- 1.1.18. The *Contractor* notifies the *Service Manager* 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 *Contractor* provides the *Service Manager* 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 *Service Manager*.

1.1.20. On request, the *Contractor* provides to the *Service Manager* all necessary information to demonstrate the *Contractor* compliance with this annex.

1.1.21. The *Contractor* promptly provides all assistance and information requested by any Supervisory Authority or required by the *Service Manager* 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 *Contractor* 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 annex.
- 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 annex.

The *Contractor* makes these records available to the *Service Manager* promptly on request.

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

- notifies the *Client* in writing of the intended Sub-Processor and processing,
- obtains the written agreement of the *Service Manager*,
- 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
- provides the *Service Manager* with such information regarding the Sub-Processor as the *Service Manager* may reasonably require.

1.1.24. The *Service Manager* may, at any time, revise this annex 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. A failure to comply with this annex is treated as a substantial failure by the *Contractor* to comply with its obligations.