

**National Highways Limited**

**Scope**

**Data Protection**

**Annex 08**

**CONTENTS AMENDMENT SHEET**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Issue No.** | **Revision No.** | **Amendments** | **Initials** | **Date** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**LIST OF CONTENTS**

1 DATA PROTECTION 4

1.1 Data Protection 4

2 DATA PROTECTION (SCHEDULE A) 8

2.1 Schedule A – Processing, Personal Data and Data Subjects 8

|  |  |
| --- | --- |
| DATA PROTECTION | |
| Data Protection | |
|  | For the purposes of the contract and the Data Protection Legislation:   * for the purposes of this Annex only the *Client* is the Data Controller, and * the *Consultant* is the Processor and * this Annex and schedule A (data protection) together constitute a data processing agreement where required by the Data Protection Legislation. |
|  | 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. |
|  | 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. |
|  | 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. |
|  | 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). |
|  | Without prejudiceto paragraph 1.1.2 the *Consultant* processes the Data only in accordance with the instructions of the *Client* unless the *Consultant* is required to process Data for other reasons under the laws of the United Kingdom and 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. |
|  | The *Consultant* immediately informs the *Client* if it believes that an instruction infringes the Data Protection Legislation or any other applicable law. |
|  | The *Consultant*   * 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 *Consultant* ensures its processing is in accordance with the Data Protection Legislation and protects the rights of Data Subjects. |
|  | 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 Security Incident. Acceptance (or a failure to reject) by the *Client* does not amount to approval by the *Client* of the adequacy of the Protective Measures. |
|  | The *Consultant* ensures that all persons authorised to process Data are bound by obligations equivalent to those set out in this Annex and are aware of the *Consultant’s* obligations under the contract and the Data Protection Legislation. |
|  | 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. |
|  | Not used. |
|  | 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 Access Request. |
|  | The *Consultant* 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. |
|  | The *Consultant* 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 Access 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 Data Subject Access Request within the time limits set out in the Data Protection Legislation. |
|  | 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.* |
|  | 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, the United Kingdom or a member state of the EEA to which the *Consultant* is subject that requires Data to be retained. |
|  | The *Consultant* 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. |
|  | 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 and in accordance with the instructions of the C*lient*. |
|  | Onrequest the *Consultant* provides to the *Client* all necessary information to demonstrate the *Consultant’s* compliance with this Annex. |
|  | The *Consultant* 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. |
|  | The *Consultant* 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 paragraph1.1.9 of this Annex.   The *Consultant* makes these records available to the *Client* promptly on request. |
|  | Before allowing any Sub-Processor to process any Personal Data related to the contract, the *Consultant*   * 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. |
|  | The *Client* may, at any time revise this Annex by replacing it with any applicable data controller to processor standard provisions or similar terms forming part of an applicable certification scheme. |
|  | The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. |
|  | Each Party designates its own Data Protection Officer if required by the Data Protection Legislation. |
|  | Not Used |
|  | A failure to comply with this Annex is treated as a substantial failure by the *Consultant* to comply with its obligations. |
| DATA PROTECTION (SCHEDULE A) | |
| Schedule A – Processing, Personal Data and Data Subjects | |
| This Schedule is 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 is taken by the *Client* andat 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 are to 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 Data Controller and the *Consultant* is the Processor in accordance with paragraph 1.1.2 of this Annex. | | Subject matter of the processing | The processing is needed in order to ensure that the Processor can effectively provide the *Service*. | | Duration of the  processing | Throughout the term of the s*ervice* | | Nature and purposes of  the processing | The nature of the processing means any operation such as collection, recording, storage, use, disclosure by transmission | | Type of Personal Data | Business contact details of *Consultant* personnel  Business contact details of any directors, officers, employees, agents, consultants and contractors of the *Client* (excluding the *Consultant’s* personnel) engaged in the performance of the *Client’s* duties under this agreement | | Categories of Data  Subject | Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers | | 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 | Data will be retained for the duration of the contract term | | |