**Data Protection Due Diligence Questionnaire**

As a Data Controller, Sustrans must only appoint data processors who can provide ‘sufficient guarantees’ that the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 will be met and that the rights of data subjects will be properly protected. This means that Sustrans needs to carry out due diligence checks before contracting and as part of contract monitoring with all its providers and contracted companies.

**The following questions should be answered with regard to any personal data or sensitive personal data held in respect of this contract.**

| **8.X** | **UK General Data Protection Regulation (UK\_GDPR) and the Data Protection Act 2018** | **Response** |
| --- | --- | --- |
| **a.** | Please provide a valid and up to date notification (Registration Number) with the Information Commissioner’s Office (ICO) that covers all personal data processing arrangements.   1. Registration Number      1. Reason for answering ‘No’ | Yes  Please provide details at (i)  No  Please explain why at (ii) |
| **b.** | Please provide details of your Data Protection Officer.   1. Name      1. Job title      1. Email      1. Reason for answering ‘No’ | Yes  Please provide details at (i), (ii) and (iii)  No  Please explain why at (iv) and provide details at b(i). |
| **b(i).** | Please provide details of your organisation’s contact for data protection matters if different to the DPO.   1. Name      1. Job title      1. Email | |
| **d.** | Are you able to provide data protection, data security and privacy policies in place within your organisation which meet current ICO recommended codes of practice?  **Please provide a copy of these policies.**   1. Reason for answering ‘No’ | Yes  No  Please explain why at (i) |
| **e.** | Are you able to provide details of privacy notices including online and published required UK GDPR documentation regarding processing etc.?   1. Relevant URL to your website      1. Reason for answering ‘No’ | Yes  Please provide relevant URL at (i)  No  Please explain why at (ii) |
| **f.** | Are you able to provide policies and procedures for handling data subject rights? (We note that if you are a data processor for Sustrans we will be responsible for handling such requests for data processed under the contract.)  **Please provide a copy of these policies.**   1. Reason for answering ‘No’ | Yes  No  Please explain why at (i) |
| **g.** | Are you able to provide a documented process and policy for managing and investigating personal data breaches, which meets UK\_GDPR requirements?  **Please provide a copy of these policies.**   1. Reason for answering ‘No’ | Yes  No  Please explain why at (i) |
| **h.** | **Employees**  Are you able to provide details of your documented processes for recruitment to check the identity and reliability of employees? For example, by obtaining references, checking qualifications, ensuring they are checked with the Disclosure and Barring Service (where appropriate).   1. Reason for answering ‘No’ | Yes  No  Please explain why at (i) |
| **i.** | **Training**  Are you able to provide details of your mandatory data protection (induction and refresher) training for all employees?  **Please provide a copy of any training material**   1. Reason for answering ‘No’ | Yes  No  Please explain why at (i) |
| **j.** | **Third Party organisation**  Will you use a 3rd party e.g. sub-contractors, partner organisations etc. to deliver this contract?  If yes, are you able to provide the security and data protection processes in place with those 3rd parties to handle council data on your behalf? Do you have processes to ensure reliability of the organisation, due diligence checks to ensure awareness of data protection, security and confidentiality of personal data, appropriate sub-contractor contracts.   1. Reason for answering ‘No’ | Yes  No  Yes  No  Please explain why at (i) |
| **k.** | **Organisational and technical measures to ensure data security**  To enable Sustrans to be satisfied that appropriate levels of Data Security are in place, are you able to provide details of password and access policies, encryption installed on mobile devices, appropriate security systems etc.? **Please provide a copy of these policies.**   1. Reason for answering ‘No’ | Yes  No  Please explain why at (i) |
| **l.** | **Storage and processing of data**  Do any of the systems or processes you use allow for the storage or processing of data outside of the UK? This includes disaster recovery/back up servers and IT system support based abroad.   1. If ‘yes’ the countries involved and the relevant systems/processors | Yes  Please provide details at (i)  No |
| **m.** | **Breach of data security or data protection**  Have you had **any** data security or data protection incidents (personal data breaches) in the past 2 years for which you have undertaken an investigation, whether or not they were reported to the ICO (or other supervisory authority if occurred in EU)?   1. Please provide additional information below, outline the circumstances and data involved, nature of the breach, including whether they were reported to the ICO (or other supervisory authority if occurred in EU), what action (if any) the ICO (or other supervisory authority if occurred in EU) took and whether any incidents have been repeat occurrences. | Yes  Please provide details at (i)  No |

**Pass/Fail assessments**

|  |  |
| --- | --- |
| **Question Number** | **Assessment method** |
| **8.Xa – 8.Xm** | **Pass** – If you have provided information that demonstrates your organisation can provide ‘sufficient guarantees’ that the requirements of the UK\_GDPR and the Data Protection Act 2018 will be met and that the rights of data subjects will be properly protected.  **Fail** – If you have not provided information that demonstrates your organisation can provide ‘sufficient guarantees’ that the requirements of the UK\_GDPR and the Data Protection Act 2018 will be met and that the rights of data subjects will be properly protected.  Providing details of breaches under 8m will not necessarily result in a ‘fail’. Each situation will be considered on its merits and discussed with our Information Rights Team as required. |