**Passenger Transport – Privacy Impact Assessment (Ref: 2017/004)**

**Provider’s Full Name:**

* + - 1. **Storage, Access, Retention and Disposal**

|  |  |
| --- | --- |
| **5.1 How will the information be stored (electronically or manually) and where?** |  |
| **5.2 Who will access to the personal data/sensitive personal data/sensitive business information?** |  |
| **5.3 How will the access be managed/ determined?** |  |
| **5.4 How long will the information be retained? Please state the legal justification where applicable.** |  |
| **5.5 What process do you intend to have in place to review retention date and in particular ensure personal data is not kept longer than necessary?** |  |
| **5.6 What disposal arrangements do you have in/intend to have in place for the personal data/sensitive personal data/sensitive business information?** |  |

* + - 1. **Technical information- For electronically held Information**

|  |  |
| --- | --- |
| **6.1 Please state the location of where the information or the application will be held? I.e. on the, desktop, shared drives, application server, hosted on internet only, hosted on intranet, etc.** |  |
| **6.2 Will the application be accessed by members of the public? Please state how (i.e via public web portal, via access Council network i.e. not web portal based).** |  |
| **6.3 If the information is held on an application or a database, please state the name of the application/database?** |  |
| **6.4 How will the application be supported by (internally by ICT or vendor)?** |  |
| **6.5 Do you intend to have an SLA in place for support?** |  |
| **6.6 Will the application or database have an interface with another system? Please state the system(s)** |  |
| **6.7 Do you intend to have a backup regime in place for the application?** |  |
| **6.8 Do you intend to have a system/hardware maintenance agreement with the vendor/ICT?** |  |

* + - 1. **Information Security**

|  |  |
| --- | --- |
| **7.1 Please state the technical security controls you intend to have in place for electronically held information?**  **( Legislative or Compliance requirements)** |  |
| **7.2 Please state the physical security controls you intend to have in place for manually and electronically held information?** |  |
| **7.3 Will the information be saved on a removable media, such as a CD, USB, or hand held device? If so what technical and physical security do you intend to apply to it?** |  |
| **7.4 Please state the technical and physical security controls the 3rd party/vendor has in place, if the application is being hosted off off-site/by the vendor. ( What accreditations they have)** |  |
| **7.5 Please state who (the departments) will be given access to the information?** |  |
| **7.6 What auditing do you intend to have in place for transactions carried out on the information and access?** |  |
| * 1. **Please detail all the security Arrangements’ in place or you will have in place (Technical , Organisational and Physical)**   **Includes:-**   * **Technical** * **Systems** * **Office Security** * **People Management** * **Security when Transferring/Migrating** * **DR** * **Patching (Roadmap)**   **All Security arrangements must be appropriate for the classification of the Information.** |  |

* + - 1. **3rd Party access**

|  |  |
| --- | --- |
| **8.1 Will the information be disclosed/accessed by a 3rd Party including for vendor support?** |  |
| **8.2 Please state the reason for disclosure/access and whether it is necessary in order for the project or process to succeed?** |  |
| **8.3 Would any such disclosure / access be systematic or Ad-hoc?** |  |
| **8.4 Can you guarantee that only adequate and relevant information will be disclosed/ accessed by the 3rd party and that the no excessive information will be disclosed/ accessed?** |  |
| **8.5 Will any processing of the manual or electronic information be carried out off-site by a 3rd Party?** |  |
| **8.6 Please state whether the 3rd party is registered with the Information Commissioner’s Office and whether they have a Data Protection Policy, if the personal data/sensitive personal data is being processed by 3rd party?** |  |
| **8.7 What processes will be used to ensure that**  **Personal data/sensitive personal data/business sensitive information is not kept longer than necessary by 3rd Party/ Vendor and disposed of securely?** |  |

## 10. Overseas Transfer - Adequate Levels of Protection

|  |  |
| --- | --- |
| **10.1 Are you transferring personal data to a country or territory outside of the EEA?** |  |
| **10.2 What are the types of data are transferred? (eg contact details, employee records)** |  |
| **10.3 Are sensitive personal data transferred abroad? If yes please provide details.** |  |
| **10.4 What are the main risks involved in the transfer of personal data to countries outside the EEA?** |  |
| **10.5 Are measures in place to ensure an adequate level of security when the data are transferred to another country?** |  |
| **10.6 Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?** |  |