**Introduction**

The UK GDPR requires that any contracted arrangements for processing personal data on our behalf that we have with a company / organisation are suitable and capable of protecting personal and special category data. Hence, it is important that we ensure any agreements that we might already have with a company / organisation or are about to put in place, are adequate.

You are requested to complete this questionnaire on behalf of your company / organisation. The completed questionnaire will be reviewed by us to ensure arrangements are compliant with the UK GDPR. Once our review is complete and we are satisfied with arrangements, we will confirm that decision and record details of arrangements in our Record of Processing Activities (RoPA).

Please contact us if you have any questions or queries regarding this request. If you need to secure this return then please do so using encryption.

**Details**

|  |  |
| --- | --- |
| **Name of Company / Organisation:** |  |
| **Service Provided:**  |  |
| Does this service involve processing special category data?  |  |

**Accountability**

|  |  |  |
| --- | --- | --- |
| **Question** | **Y/N** | **Details** |
| Do you act purely on our instructions in terms of how and why you process our data?If no, detail those other instructions.  |  |  |
| Do you reuse any of our data for your own purposes (e.g. analytics, advertising, profiling, R&D). If yes, provide details of how data is reused and other measures implemented (e.g. anonymisation) |  |  |

**Assurance**

| **Question** | **Y/N** | **Details** |
| --- | --- | --- |
| Please confirm that your organisation complies with the UK GDPR and DPA 2018 and all other applicable legislation with respect to the processing of personal data.If you are registered with the ICO please supply your ICO registration number. If you have not registered please explain why. |  |  |
| Do you have a Data Protection Officer or someone else designated to take responsibility for data protection?Please supply contact details. |  |  |
| Do you have a register of personal data you process for us, the activity/purpose, and a general description of the security controls in place to protect our data? |  |  |
| Is any the processing of our data sub contracted out at any point? |  |  |
| Is any of our data transferred outside of the European Economic Area at any point? |  |  |
| If yes to the above question, then detail what countries it is transferred to and any controls in place (e.g. standard contract clauses, binding corporate rules) |  |
| In your company / organisation, which data protection and related policies and procedures are in place? (e.g. data breach reporting, data retention, subject access request, cyber security).How often are these documents reviewed? |  |
| Is data protection training provided to relevant staff?If yes, provide details (including when, how and the content of that training) |  |  |
| Describe what access controls are in place in terms of physical security and logical security on your systems that process our data. |  |
| Provide details of your organisation's technical and organisational measures that ensure any personal data you hold is kept in accordance with the requirements under UK GDPR.Tick the information security certificates and registrations you company / organisation holds. * PCI-DSS
* ISO27001
* Cyber Essentials
* Cyber Essentials Plus

Other(s) / equivalent certifications and registrations of another country (please state, if applicable) |  |
| Do you audit and/or risk assess your security controls? |  |  |
| Do you conduct any additional security checking - vulnerability scanning, IT Health Checks, or penetration tests?When did your company / organisation last conduct a check / test?  |  |  |
| Do you apply encryption, pseudonymisation and/or data minimisation to the processing of our data?  |  |  |
| Describe your approach to applying patches and updates. |  |
| Describe any other security measures that are in place to protect our data (e.g. anti-virus/malware etc) |  |
| How and where is data backed up? |  |
| How long is data retained for?  |  |
| Describe your approach to disposal of personal data (both equipment and paper) |  |
| In the event of a data breach, what is the process? |  |
| How will you notify us if a breach occurs? |  |

|  |  |
| --- | --- |
| **Completed by (Name and Role):** |  |
| **Date:** |  |