**Contracts checklists**

|  |  |
| --- | --- |
| **Date** |  |
| **Author** |  |
| **Are you the Controller or the Processor?** |  |
| **Activity / Contract being reviewed** |  |

Under the GDPR, when processing will be carried out on behalf of a Data Controller by a Data Processor there must be suitable contract in place that is binding on the processor with regard to the controller and includes certain information in order for it to be deemed compliant. Please note it is the responsibility of both parties to ensure the following is therefore included:

**Mandatory requirements**

☐ Only act on the controller’s documented instructions;

☐ Impose confidentiality obligations on all personnel who process the relevant data;

☐ Abide by the rules regarding appointment of sub-processors and the rules about transfers of personal data outside the EEA;

☐ Implement measures to assist the controller in complying with the rights of data subjects;

☐ Assist the controller in obtaining approval from data protection authorities (the ICO in the UK) where required;

☐ At the controller’s election, either return or destroy the personal data at the end of the relationship (except as required by EU or member state law);

☐ Ensure the security of the personal data it processes;

☐ Provide the controller with all information necessary to demonstrate compliance with the GDPR and allow for and contribute to audits (including inspections) conducted by the controller or another auditor mandated by the controller;

☐ Assist the controller in ensuring compliance with the controller’s security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and, when necessary, consultation with the data protection authorities, taking into account the nature of processing and the information available to the processor;

☐ Inform the controller if an instruction from the controller infringes EU data protection law

**Must also contain:**

☐ The name and contact details of the processor and the controller and, where applicable, of their data protection officer(s);

☐ The subject matter, nature and purpose, or purposes, of the data processing;

☐ The duration of the processing;

☐ The types of personal data to be processed and categories of data subjects;

☐ Where possible, a general description of the technical and organisational security measures protecting the personal data

☐ Indemnities, caps of liability in the event of breach of data processing obligations and mandatory insurance may also be found in some Data Processing Agreements but they are optional.

Following completion

☐ The contract has been signed by suitable personnel on behalf of all parties

☐ The contract and any associated paperwork has been stored securley