| **Data Processor (Supplier) - Contract Checklist** | |
| --- | --- |
| Data Processors are organisations that process (use/manage/hold) personal data on behalf of the University. The law requires that all contracts with data processors include the terms set out below.  **INSTRUCTIONS FOR USE:** This checklist should be completed by the person responsible for the project with the support of the supplier (data processor). A Data Protection Impact Assessment (DPIA) and/or supplier checklist (see Appendix 1) may also be required. Please then contact the Data Protection Officer: [**DPO@essex.ac.uk**](mailto:DPO@essex.ac.uk) for approval/to review any gaps.  Please copy and paste below the relevant clause(s) against each requirement: | |
| Please embed a copy of the full contract here: |  |
| Please first outline (or reference a document which outlines):   * the subject matter * the duration * the nature and purpose of the processing * the type of personal data involved * the categories of data subject * the controller’s obligations and rights |  |
| “The processor must only act on the controller’s documented instructions, unless required by law to act without such instructions” |  |
| “The processor must ensure that people processing the data are subject to a duty of confidence”  NB: People means employees, contractors or anyone working for the processor |  |
| “The processor must take appropriate measures to ensure the security of processing” |  |
| “The processor must inform the University of any actual or potential data breach immediately and no later than 24 hours after becoming first aware of any incident which does or may include personal data of which the University of Essex is a data controller” |  |
| “The data processor must provide any assistance required by the University in order to comply with data subjects rights” |  |
| “The processor must only engage a sub-processor with the controller’s prior authorisation and under a written contract” |  |
| “The processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights” |  |
| “Taking into account the nature of processing and the information available, the processor must assist the controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments” |  |
| “The processor must delete or return all personal data to the controller (at the controller’s choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage” |  |
| “The processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to be assured that they are both meeting their obligations under data protection law” |  |

**Appendix 1 - Data Protection Supplier Assessment**

Questions for suppliers with access to personal data

| Question | Response |
| --- | --- |
| What will be the nature of your organisation’s relationship with the University? | ☐ Separate Data Controller  ☐ Data Controller in common  ☐ Data Processor  ☐ Other, please specify |
| Please supply the contact details of your Data Protection Officer/representative |  |
| Does your organisation have an Information Commissioners Office (ICO) registration number? | ☐ Yes, please supply:  ☐ No |
| Does your organisation have any information security accreditations? | ☐ Cyber Essentials  ☐ Cyber Essentials plus  ☐ ISO27001  ☐ Other, please specify: |
| Do all employees in your organisation (who would have access to personal data) have a contract that includes a confidentiality clause? |  |
| Do your employees receive any data protection training? | ☐ Yes  ☐ No |
| Do you have policies in place to protect personal data?  Please supply a copy of the policies as supporting information. | ☐ Data Protection Policy  ☐ Information Security Policy  ☐ Records management Policy  ☐ Other, relevant document: |

Guidance:

Personal data is any data of the University’s staff, students or others which could identify an individual e.g., name, address, student number, ethnicity, medical information etc.