Checklist for Data Processing Agreements with "Data Processors"
Articles 28 & 32

In order for any processing to take place by a third party it must be "governed by contract" to be compliant with data protection legislation. The following must be included in the contract/agreement:

1) Details of parties including ICO Registration numbers (where applicable)
2) Defining of Data Processor relationship
3) Define legislation and terms used, particularly confidential information and sensitive/personal data (From May 2016 all data sharing agreements should reference the General Data Protection Regulation 2016 (GDPR) and UK Data Protection Act 2018)
4) Processors: Define and detail exact services to be provided and include service standards/SLAs. Article 28 specifies:
    a) detail the purpose of processing and subject matter
    b) type and category of personal data being processed
    c) duration of processing including final disposition (destroyed or returned)
5) Define lawful bases for each party for processing including additional conditions for sensitive personal data if relevant (for processors this will be 'under [this] contract')
6) Define term of agreement and period for notice to terminate
7) State rights and obligations of Data Controller (Edinburgh Napier University) (to provide instructions for processing and the data to be processed)
8) Ownership of the data lies with the University
9) State obligations of Data Processor
    a) Full authority/power to process personal data
    b) Will process only on the written instructions of the Controller
    c) Will assist promptly with all requests from Data Subjects exercising their rights under data protection legislation without further cost
    d) No disclosure of confidential/personal data to any other third parties without the consent/instruction of the Data Controller (procedure for providing instructions to be agreed)
    e) Data Controllers to be advised promptly of any disclosures required by law
    f) Data Controller to be fully indemnified against any breaches which occur due to a fault on the part of the Data Processor
    g) Breaches:
        i) Data Controller to be fully indemnified against any breaches which occur due to a fault on the part of the Data Processor
        ii) Any data security incident or breach of data protection legislation must be reported promptly to the Data Controller, within 12 hours of discovery
        iii) Assist with any investigations and notifications where necessary
    h) The information is the property of the Data Controller and arrangement under 4)c) must be provided without charge
    i) The Data Processor must "demonstrate compliance" with the GDPR, in particular providing details of organisational and technical measures (Article 32) which ensure appropriate security of confidential and personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, e.g.
        i) Organisational measures:

(1) Employee vetting,
(2) Adherence to confidentiality clauses by contract or legislation
(3) Requirement for regular data protection training (annual preferably, biennial at the minimum)
(4) Only those employees who need access to the data to process it will have permission to do so.

ii) Appropriate organisational policies and procedures in place e.g. data protection policy, information security policy (manual and electronic), business continuity policy/plan, breach identification/reporting policy/procedure

iii) Details of the security measures in place at all stages of the processing done on behalf of the University e.g. collection, storage, transmission, use, retention, destruction (Governance Services can provide a questionnaire)

iv) Provide or assist in the undertaking of a Privacy Impact Assessment if necessary

j) Data not to be processed in any way outside the EEA, including back-ups without written agreement from the University prior to such processing. Preferably data will be processed in the UK.

k) Data processing not to be subcontracted to another party without the express written consent of the University (who may which to clear any such contractors separately). Sub-processors are to be under the same obligations as the main processor, set out in written contracts. Existing sub-contracted processors must be agreed prior to approval and any changes to be notified throughout the term. Sub-contracted processors must "demonstrate compliance" with the GDPR, in particular providing details of organisational and technical measures which ensure appropriate security of confidential and personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, e.g.

i) Employee vetting, adherence to confidentiality clauses in contracts or agreements, and requirement for regular data protection training (annual preferably, biennial at the minimum). Only those employees who need access to the data to process it will have permission to do so.

ii) Appropriate organisational policies and procedures in place e.g. data protection policy, information security policy (manual and electronic), business continuity policy/plan, breach identification/reporting policy/procedure

iii) Details of the security measures in place at all stages of the processing done on behalf of the University e.g. collection, storage, transmission, use, retention, destruction

iv) Assists with data subject rights requests where appropriate and necessary, without charge

l) Data Processor will allow the University to conduct appropriate audits to ensure GDPR compliance or SLA standards are being maintained.

m) Confidentiality must extend beyond the term of the agreement/contract

n) Processor is liable for breach of the legislation caused by processing outside of the University's instructions or any other breached caused by a fault of the processor or any of their sub-processors

10) Confidentiality – general clause

11) Rights:

a) Privacy notice and arrangements for dissemination to be detailed

b) Ensures the protection of the rights of Data Subjects and will assist where necessary in the exercise of those rights without charge

12) Confidentiality – general clause

General

13) Termination of agreement/contract and consequences of termination
14) Assignment and subcontracting
15) Notices
16) Severability
17) Variation
18) Waiver & Indemnities
19) Governing Law
20) Entire agreement
21) Further assurances
22) Witnessed signatures