Checklist for Data Sharing Agreements with other "Data Controllers" Article 26

1) Details of parties including ICO Registration numbers (where applicable)
2) Defining of Data Controller/Data Controller relationship, joint or other variation
3) Define legislation and terms used, particularly confidential information and sensitive/personal data (General Data Protection Regulation 2016 (GDPR) and UK Data Protection Act 2018)
   Controllers: Define arrangements between the parties:
   - determine respective roles and responsibilities
   - which party is collecting the data (who's collecting/processing what)
   - whose data is being collected/processed and what categories of data
   - a broad description of each party's purposes for processing, linked to
   - lawful bases for each party for processing including additional conditions for sensitive personal data if relevant
   - the arrangements for the provision of privacy notice/s;
     - these can be joint or individual(organisation) notices
     - must refer to the arrangement the agreement references
     - preferably disseminated at point of data collection, and
     - include contact details for data subjects to exercise their other rights conferred under the legislation
4) Define term of agreement and period for notice to terminate
5) Each party to confirm it has full authority/power to process personal data.
6) Breaches:
   a. Any data security incident or breach of data protection legislation must be reported promptly to the Data Controller, within 12 hours of discovery
   b. Assist with any investigations and notifications where necessary
   c. (Optional) Each party can indemnify the other against any breaches which occur due to a fault on their part
7) Retention periods for data to be defined
8) Each party to confirm they "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.
   a. 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.
   b. 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
   c. 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
   d. Provide or assist in the undertaking of a Privacy Impact Assessment if necessary
9) Confidentiality must extend beyond the term of the agreement/contract
10) Confidentiality – general clause

General

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