PENNINGTONS MANCHES

Checklist of data protection considerations

Consultancy arrangements

Note: this checklist is intended to provide a high level list of issues to be considered from a data protection perspective when appointing a consultant. It is not intended to be exhaustive and is not a substitute for legal advice.

1. Who else will the Consultant be sharing the personal data with?	If the Consultant is sharing personal data with a third party: • Does the personal data need to be shared by the Consultant or could the objective be achieved without sharing personal data (e.g. by anonymising or redacting)? • Does the sharing meet at least one of the conditions of processing (e.g. is it required for a contract, to comply with a legal obligation or necessary for the Consultant to provide services)? If special category personal data is being shared has at least one of the special conditions of processing been met? • Is there any third party processing personal data on behalf of the Consultant (i.e. Will there be sub-processors)? If so, this should be addressed in any contractual arrangement to meet the requirements set out in Article 28 (see below) • Does the sharing involve the transfer of data outside the EEA? If so, one of the approved transfer mechanisms must be used (see below).
2. Does the Consultant, or the Consultant's processors, transfer data outside the EEA?	• Which of the approved transfer mechanisms set out in Articles 44 to 49 of GDPR is being used (i.e. one of the appropriate safeguards (adequacy finding/privacy shield (if to US)/model

	clauses/binding corporate rules) or one of the permitted derogations))? • Are there any other national laws (e.g. in country to which the data will be transferred) which might have an impact?
3. What security measures does the Consultant have in place?	• Will personal data be secure throughout its processing? Are the security measures appropriate to the likely risk to data subjects if the data was lost, stolen or disclosed to unauthorised individuals? • Does the Consultant have procedures in place to enable it, if required, to report a data breach to data protection authorities within 72 hours?
4. What insurance cover does the Consultant have?	• Does the insurance cover costs associated with GDPR non-compliance and resulting business disruption losses to our satisfaction?

Nature of the data sharing

5. Is this a '*controller to controller*' or '*controller to processor*' arrangement?	• If the Consultant is processing personal data on our behalf (i.e. a 'controller to processor' arrangement) then a contract must be put in place between the processor and the Consultant containing the specific provisions set out in Article 28 of the GDPR (see below) • If personal data is shared with the Consultant for reasons other than data processing on our behalf where the Consultant will have a determining role in relation to the purposes or means of processing (i.e. a 'controller to controller' arrangement) are measures in place to comply with the requirements of GDPR (see below)?
6. Who are the data subjects?	• Do they know you are sharing their personal data with the Consultant (and, if applicable, any third parties with whom the Consultant is sharing their personal data)? • Are appropriate privacy notices setting out, in clear and plain language, all of the information required by Articles 12 to 14 GDPRin place?

	• Does the Consultant have processes in place to enable data subjects to exercise their data subject access rights? • Do you have the data subject's consent to share the data, if applicable?

Engagement of the Consultant

7. If the consultant is a processor	• Have you received 'sufficient guarantees' from the Consultant that it can implement technical and organisational measure to meet the requirements of GDPR? • Do you have a written contract with the Consultant that includes the requirements set out in Article 28 of the GDPR? A summary of the requirements of Article 28 include the following: • Subject matter of processing • Duration of processing • Nature and purpose of the processing • Type of personal data • Categories of data subject • Engagement of subprocessors • Transfers outside the EEA • Commitment to confidentiality • Deletion and return of personal data at the end of the processing • Audits and inspections
8. If the consultant is a controller	• Does your contractual arrangement provide for cooperation over data subject rights (i.e. in the event of a data subject access request or a data breach)? • Are you confident the Consultant is committed to and able to meet all the requirements of GDPR (including data security, record keeping and implementing appropriate data protection policies and procedures)?