Key Areas for Consideration In Data Processing Contracts

Data processing means "*obtaining, recording or holding the data or carrying out any operation or set of operations on data*"[1]. 3rd parties providing these services on behalf the University become data processors but the legal obligations around data protection remain with the University. The University could be fined up to £500k by the Information Commissioner's Office for breaches for data protection.

Information on University information classes and outsourcing processing services can be found on http://www.go.warwick.ac.uk/gov/informationsecurity

- Has the UoW Project Manager or lead sought Data Protection and Information Security advice from the Secretary to Council's Office? If not, this must be obtained before proceeding to contact approval. The SCO can help ascertain whether potential providers can provide appropriate security for University data.

- Where (geographically) the data is processed. If it is outside Europe (formally, outside the EEA) and in a country not recognised by the Information Commissioner[2] as providing adequate levels of protection and not stored in the USA under the EU-US Privacy Shield Framework, then you should not use the service.

- If the data is processed with a US company subject to the Federal Trade Commission[3], you need to be aware that the company will transfer your data to the USA when compelled (or sometimes simply requested) to do so. As non-US citizens, we do not have the same levels of protection with respect to our data as US citizens do when data is stored in the USA.

- Can the provider confirm that the UoW data will only be used for the agreed purposes (i.e. what you have consent for from the individuals/activities to which the data relates)?

- Whether the personal and sensitive data is (strongly) encrypted when stored, transferred and processed and whether strong authentication and limited access control will be in place to ensure confidentiality.

- Will the provider use any sub-contractors to process your data, can the company confirm that they will act as UoW's representative with sub-contractor(s), working in the best interests of UoW at all times including timely payments, review and compliance to of terms of licence particularly when amended, reporting of incidents, service level agreements and remedies for failing to achieve key performance criteria?

- How and when you can access your data during the contract? Of particular note is the UoW's obligation to respond to Freedom of Information requests within the 20 working days limit or 40 days for responses to a Subject Access Request and even if the data is held outside of the UoW, the law still regards the University as holding the data.

- Can the company confirm that if/when the services are terminated all UoW information within its or any sub-contractor(s) possession will be securely removed and deleted from all systems OR returned to University?

- What service levels are provided and are they adequate to your needs? What disaster recovery and business continuity plans are in place to ensure continued availability of the service?

- What are the company offering in terms of liability for loss, misuse or damage of University data? Whilst the University's data may be one small part of the provider's activities and therefore high liability is not attractive to them, loss or damage to UoW data could pose potentially serious reputational damage for the UoW so it is important that liability appropriate to the risk to the University is secured.

- How will breaches of security affecting University data be reported and managed in liaison with the University? Assurances should be given around timely and open reporting.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/
[2] https://ico.org.uk/
[3] http://www.ftc.gov/