

**General Data Protection Regulation**

**Supplier Questionnaire**

|  |  |  |
| --- | --- | --- |
|  | | **Response** |
| 1 | Please confirm that your organisation complies with the General Data Protection Regulations 2018 and all other applicable legislation with respect to the processing of personal data.  If you are registered with the ICO please supply your ICO registration number. If you have not registered please explain why. |  |
| 2 | Is the processing of personal data on behalf of Leeds Beckett University a significant feature of this contract. | If NO, no further checking required  If YES, at award stage supplier to complete questions 3 – 14 |
| 3 | If you have answered YES to question 2 please provide details of the nature of the contract you will be providing, the types of personal data being processed and any special category data. |  |
| 4 | The University needs to be satisfied that you have appropriate cybersecurity certifications in place.  Provide details of your organisation's technical and organisational measures which ensure that any personal data you hold is kept in accordance with the requirements under GDPR.    Tick which Information Security certifications and registrations you hold (tick which apply)   * PCIDSS * ISO27001 * DPA/ICO * Cyber Essentials * Cyber Essentials Plus   Other(s) / equivalent certifications and registrations of the relevant EU/EEA member state (please state, if applicable)  (Maximum of 250 words) |  |
| 5 | Is data protection training provided to relevant staff?    If yes, please provide details (including when, how and the content of that training) |  |
| 6 | In your organisation which data protection and related policies and procedures are in place? (e.g. data breach reporting, data retention, subject access request, data security, cyber security).   How frequently are those policies reviewed? |  |
| 7 | Do you have a data protection officer or someone else who has been designated to take responsibility for data protection?  Please supply contact details. |  |
| 8 | In the last 3 years, have there been any breaches of your data protection policy (or any related policies), or your DPA/PCI-DSS registrations?    If yes, please provide details (including action taken to avoid any repeat breach) |  |
| 9 | In the last 12 months have you received any complaints from data subjects in respect of your treatment of their personal data?    If yes, please provide further information. |  |
| 10 | In the last 12 months have you either reported an incident to the ICO within your organisation or been subject to any action from the ICO?    If yes, please provide further information |  |
| 11 | Are all staff, agents and key subcontractors used to delivering similar contracts subject to contractual obligations of confidentiality which comply with GDPR?    *[If yes, please explain how these obligations comply with GDPR and provide copies of relevant confidentiality and data processing clauses used in the contracts that you have with those people/organisations]* |  |
| 12 | If you are proposing to sub-contract any part of the work which involves the processing of Personal Data, that you will carry out on our behalf, do you have a contract in place with your sub-contractor that includes data processing obligations?  Please provide a copy of the relevant clauses. |  |
| 13 | Do you have in place technical and organisational measures to assist your clients with their obligations as a data controller in respect of Subject Access Requests and the other data subject rights under GDPR?    If yes, please provide further information including how quickly you are able to respond. |  |
| 14 | Will you, or any third parties acting on your behalf, be processing any of our personal data outside of the EEA (except the United Kingdom)?  If yes, please confirm how you will fulfil the obligation of adequate protection in respect of the personal data you will process and set out how you will fulfil the obligation of adequate protection in respect of that personal data. |  |

NOTES:

**When does GDPR apply to a contract?**

GDPR applies when the contract includes the processing of personal data. Personal data is defined as ‘any information relating to an identified or identifiable individual’.

Personal data can include:

**General personal data**

* personal email addresses
* personal mobile
* NI number
* Financial details

**Special category personal data**

* racial or ethnic origin
* political opinion
* religious beliefs
* Trade Union membership
* physical or mental health condition
* Sex life and sexual orientation
* matters relating to criminal offence or court proceedings
* genetic data
* biometric data