

**MEDIUM/LARGE ORGANISATION**

**GDPR COMPLIANCE QUESTIONNAIRE**

The General Data Protection Regulation (GDPR) came into force on 25th May 2018. The GDPR applies to Controllers (who say how and why personal data is processed) and Processors (who act on the Controller’s behalf). GDPR applies to any public or private organisation accessing personal data. The key purpose of GDPR is to increase and protect the rights of EU data subjects by creating clear channels of accountability over data processing.

Further information on GDPR can be found on the Information Commissioner’s Office: <https://ico.org.uk/for-organisations/business/>

The questionnaire is intended to assess whether the bidder(s): (a) meet the requirements of the GDPR and (b) ensure the protection of the rights of the data subject.

The questionnaire assessment will be carried out through a mixture of pass/fail and scored questions. Scored questions will follow the scoring methodology set out in the tender documents. Bidders that fail any of the pass/fail questions or do not score a **minimum of 3 points in any given question** may be excluded from the process and their bid might not be further considered.

Bidders should note that:

* Suppliers will be expected to manage their own costs in relation to compliance with GDPR;
* Under the GDPR Processors now face direct legal obligations and they can be fined by the Information Commissioner’s office (ICO);
* The contract documents to be entered into by the successful supplier(s) will include specific obligations in relation to GDPR;

|  Item No# | **ITT QUESTIONS** | **Contractor answers** | **Scoring** |
| --- | --- | --- | --- |
|  | **DATA PROTECTION** |  |  |
| **1** | **The General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR”), requires all companies processing personal data to demonstrate that they meet the Regulations’ requirements. As a supplier to the Council, we will need evidence and assurance of your compliance and we will undertake periodic monitoring.**  |
| a | Please provide evidence of policies and procedures you have in place to inform staff of their responsibilities and set out the company’s standards in:Data Protection Security Incident Handling; Information SecurityRecords Management Subject Access RequestsData DisposalData Backup)Business Continuity and Disaster recovery Privacy Impact Assessment**Assessment Guidance:****Data Protection** clearly set out how is data kept safe, what are the limits to access data, roles and responsibilities, guidance for handling data]**Security Incident Handling**; [clear process, who to report to, who will investigate, Evaluation of the incident and resolution]**Information Security**[building security, access to ICT systems, ICT security, ]**Records Management** [What records are kept, who can access, how to record, safe data transfer]**Subject Access Request Procedure** [staff and user awareness, process, roles and responsibilities defined, -may need to liaise with Council]**Data Disposal procedure/policy** [retention period, safe disposal – shred / secure waste bins / electronic record / end of contract process]**Data Backup policy/procedure** **Business Continuity and Disaster recovery plan/policy** [ICT back up and how service will operate if ICT fails / needs recovery or lack of access to building] | Attachments |  Scored: [1] [2] [3] [4] [5] |
| b | Do you assess data / privacy risks? How?**Assessment Guidance:****Controllers have privacy impact assessment template** | [Yes] or [No]Attachment  | Pass/fail |
| c | **Is there a central record of processing activities?** **Assessment Guidance:****[The central record should set out data processed, purpose, condition for processing, responsible person, any ICT system, retention period]** **[if spreadsheet one entry for each process]****[NB if this contract delivers a new process for supplier, they will need to show example]** **[Should be reviewed once a year (minimum)]** | [Yes] or [No]Type | Pass/failScored: [1] [2] [3] [4] [5]  |
| d | **What are your policies and procedures in place for detecting and** **dealing with breaches? [Mandatory]** **Assessment Guidance:****[Clear processes setting out how to detect and deal with breaches]** | Type | Scored: [1] [2] [3] [4] [5] |
|  | **TECHNICAL AND ORGANISATIONAL SECURITY** |  |  |
| **2** | **In accordance with Article 32 of the GDPR, you must implement appropriate technical and organisational security measures to protect the Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed;** |
| a | **Please provide evidence that you have a level of ICT security appropriate to the risk, taking into account the harm which might result from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed in light of systems required,** **e.g.*** IT Security Controls accreditation? (PSN CoCo. And ISO27001/2 or Cyber Security Plus) [Desirable] if not, it is mandatory demonstrate compliance with (National Cyber Security Centre) NCSC 10 steps to Cyber Security:

<https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security>Other ICT security controls: If data in held in a hosted solution, demonstrate their compliance with the National Cyber Security Centre (NCSC) 14 Principles for Cloud Security<https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles>**Assessment Guidance:****[ICT security controls are in place to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access]** | [Yes] or [No][Yes] or [No][Yes] or [No][Yes] or [No]Type | Pass/Fail and Scored: [1] [2] [3] [4] [5] |
|  | **STAFF TRAINING & AWARENESS** |  |  |
| **3** | **Please provide evidence of staff training (induction and annual refresher) on Data Protection and Information Security [and, where relevant, the requirements of the data processing agreement]** |   |  |
| a | **Do the employees in your organisation receive training and awareness briefings on data protection and information security? . Mandatory*** **The Board [Mandatory],**
* **Senior management [Mandatory],**
* **Security/IT team [Mandatory],**
* **All other staff [desirable]**

**Please describe the nature of the training given, when it is given and who is responsible for carrying out training** | [Yes] or [No]Type Details | Scored: [1] [2] [3] [4] [5]  |
|  | **ORGANISATIONAL AND TECHNICAL MEASURES** |  |  |
| **4** | **In accordance with Article 32 of the GDPR, you must implement appropriate technical and organisational security measures to protect the Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed;** |   |  |
| a | * **What data access audit facilities/mechanisms are in place**?
* **(How do you check that there has been no internal unauthorised access to personal data?)** Who has access to personal information within the organisation/outside the organisation? Who authorises such access?

**Assessment Guidance:****[What data audit facilities/mechanisms are in place]** **[Access on need to know basis] [Clear role allocated]** | Type | Scored: [1] [2] [3] [4] [5]  |
| b | **What user User Identification and Authentication do you use to access to data (Mandatory requirement)****Provide details.****Assessment Guidance:****[How do users access data, password control, other authentication e.g. token generating number]** | [Yes] or [No]Type | Pass/Fail and Scored: [1] [2] [3] [4] [5]  |
| c | **Do staff using mobile/remote system have Two-factor authentication? (Mandatory requirement)** | [Yes] or [No][NA] | Pass/Fail (if applicable |
| d | **Is accredited penetration testing undertaken? (Mandatory requirement)****Assessment Guidance:****[Robustness of firewall]** | [Yes] or [No] | Pass/Fail |
| e | **Is there AES-256 bit encryption on all devices, information at rest and data in transit (Mandatory requirement**)**Assessment Guidance:****[Encryption must be applied to all OFFICIAL SENSITIVE data in transit]** | [Yes] or [No] | Pass/Fail (if applicable) |
| f | **Confirmation of where electronic data held (in house or off-site)** | [onsite] or [offsite] | Information only |
| G | **Do you destroy personal information securely? Secure destruction is Mandatory****Assessment Guidance:****[Shred /waste contractor for paper, secure destruction of ICT equipment]****[Contract specifies process and offers guarantees of security]** | [Yes] or [No]Type | Pass/fail and Score: [1] [2] [3] [4] [5] |
|  | **DATA TRANSFERS** |  |  |
| **5** | **Assurance that transfers storage and processing of Personal Data is only within the European Economic Area**  |  |  |
| **a** | Do you transfer personal data? If so explain how data is transferred? Please confirm that all data processing occurs within the EEA**Assessment Guidance:****[e.g. Encrypted email, Tracked post]** | [Yes] or [No][NA]Type | Pass/fail (if applicable) and Scored: [1] [2] [3] [4] [5]  |
|  | **MONITORING MECHANISMS** |  |  |
| **6** | **You should have plans to conduct audits of the information or processes relating to your compliance with obligations under the GDPR.**  |   |  |
| a | **Compliance with the General Data Protection Regulation is assessed annually at minimum. (Mandatory requirement)** **For example,*** **Information Security audits)**
* **Records Management audit Business Continuity and Disaster recovery plan tested**

Provide review plans**Assessment Guidance:****[Plan in place]** | [Yes] or [No} Attachment | Pass/Fail and Scored: [1] [2] [3] [4] [5] |
|  | **SUB-CONTRACTORS** |  |  |
| **a** | **Are any of your processing activities carried out by third parties (sub-processors)? If non, next section does not apply** | [Yes] or [No} | Information only |
| b | Please set out how you will monitor and ensure their compliance with GDPR. Also how you will facilitate the Council accessing this monitoring data, including direct contact with the sub-contractor if required. Provide a plan to monitor compliance in subcontractors**Are written agreements in place covering these arrangements with sub processors?****Assessment Guidance:****[Minimum monitoring should be once a year]** **[Plan in place]** | Type | Scored: [1] [2] [3] [4] [5] |