**TAPPI Checklist**

**Data Security questionnaire**

**Information required from technology suppliers to support safety and security**

This checklist aims to support health, care and housing services to capture safety and security information from technology suppliers and receive the clarity they need in order to safely begin to use such solutions, and also to provide confidence to their information governance and ICT colleagues that the right questions have been asked.

The checklist isn’t meant to be an exhaustive list of questions, but can be used as a starting point to then add on any further requirements from ICT, etc:

|  |
| --- |
| **Personal data**  Describe the nature of the data captured and transmitted by the TEC solution  *Ahead of any deployment you will be required to provide a detailed diagram of the end-to-end solution being delivered (including all servers, data centres, methods of connection).* |
|  |
| **Pseudonymisation**  How will you guarantee that pseudonymised data is not matched with an individual user or their address? |
|  |
| How will set-up / faults / repairs of units be handled to avoid matching collected data with user address? |
|  |
| **Past experience with pseudonymised user data**  How much experience do you have?  How successful has it been?  What challenges did you face, and how were these overcome? |
|  |
| **Where is data processed?**  In which country are your servers based?  Will data be transferred to, or accessed from, any countries outside the UK?  *Your organisation is expected to adhere to the National Cyber Security Centre cloud principles -* [*https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles*](https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles) |
|  |
| **Access**  Who, within your organisation, will be authorised to access the pseudonymised data, and for what reason/s?  Will access to the data be granted to any other organisation? (NB including sub-contractors) |
|  |
| **Security Measures**  Describe security measures which are used to prevent unauthorised access, accidental loss or destruction of data:   * During transmission * On your servers |
|  |
| **Accuracy and integrity of data**  Describe measures used to ensure that the data transferred to us is timely and accurate. |
|  |
| Would the Supplier retain any records after termination of the services? If so, please explain why, for how long this would be considered necessary, and describe the process for deleting these records afterwards. |
|  |
| Do you have an information governance structure in place? Describe the structure briefly, including details of who are the Supplier personnel responsible for overseeing information security and data protection governance matters?  What are their qualifications, expertise and experience? |
|  |
| How will you train your staff on your business processes, information security and data protection governance standards? |
|  |
| Please provide details of your mechanism for reporting and managing information risks, data protection breaches or data security breach incidents of any kind, including reporting loss of personal data as soon as reasonably practicable & notifying the commissioning body?  *Please provide information regarding any previous instances of breach or loss of data and reasons why* |
|  |
| What audit trails are available to monitor who accesses any relevant systems, equipment and data used to provide the services in order to ensure that processes are being followed correctly and that no information security or data protection breach has occurred?  It is expected that your organisation will provide details of the most recent penetration testing and information on any rectifying actions taken |
|  |
| Describe your vetting and background checks processes carried out on the reliability of your staff, including employees, contractors, temporary workers? This should include on recruitment and during their employment. |
|  |
| Will there be a particular team working on any solution/service provided to our organisation? Please provide brief details where appropriate of any applicable training or qualifications of key team members/ workers. |
|  |
| Is user access to the recorded information restricted by default without prior authorisation? |
|  |
| What is the rolling 12-month annualised downtime for the solution and what were the recovery times for any outages in the last 12 months? |
|  |

Prepared by the TEC Services Association for the [TAPPI project](https://www.housinglin.org.uk/Tappi).