PROCESSOR AND SUB-PROCESSOR QUESTIONNAIRE

Version 4	June 2022
Agreed by SMT	June 2022
Review date	June 2024

Background

- The UK GDPR applies to Controllers (who say how and why Personal Data is processed) and to Processors (who process Personal Data on behalf of a Controller under a contract or legally binding Data Processing Agreement).
- Where a Processor is permitted to sub-contract the processing of Personal Data it was employed by the Company to process, that sub-contractor will become a Sub-Processor.
- Processors and Sub-Processors are expected to maintain the same standards in relation to the processing and security of Personal Data as those that apply to their Controllers and Processors respectively.
- Sub-Processors thus employed must be bound by a suitable contracts or legally binding Data Processing Agreements containing the same or equivalent terms relating to Processing Personal Data as the contract between the Company and the Processor.

Questionnaire Notes

1. This Questionnaire supports Age UK East London's Data *Processing by External Suppliers Policy*.
2. The purpose of this Questionnaire is to assess whether potential Processors and Sub-Processors:
    a. meet the requirements of the Data Protection Legislation under which Processors and Sub-Processors now have direct legal obligations and penalties can be imposed by the Information Commissioner's office (ICO);
    b. meet the National Cyber Security Centre (NCSC)'s standards set out in its "10 Steps to Cyber Security".
    c. and meet the Company's standards in protecting the rights of its Data Subjects and those of its Controllers and partners.
3. Potential Data Processors and Sub-Processors should answer all questions.
4. The assessment of responses will be undertaken by Age UK East London.
5. Potential Data Processors and Sub-processors that do not meet the required standard may be unable to undertake processing of Personal Data on behalf of the Company, at least until they are able to reach the required standard.
6. Potential Data Processors and Sub-processors should note that:
    a. Data Processors and Sub-processors will be expected to manage their own costs in relation to completing this Questionnaire and any other assessment requirements required by the Company and for compliance with Data Protection legislation
    b. If they fail to meet the required standard they may be unable to undertake processing of Personal Data on behalf of the Company, at least until they are able to reach the required standard.
    c. If the contract documents to be entered into by a Data Processor or Sub-processor do not in themselves adequately describe its obligations relating to the Processing of

Personal Data in the judgement of Age UK East London, the Parties will need to enter into an additional legally binding Data Processing Agreement.

East London age UK	**Age UK East London** **Data Processing and Sub-Processing Questionnaire**	**3.1**

No	Question	Response	Guidance	Score
1	**Policies & Records** Provide evidence of your policies and procedures to inform staff of their responsibilities and set out your organisation's standards in: • Data Protection • Information Security • Records Management • Subject Access Requests • Data Disposal • Data Backup • Business Continuity and Disaster recovery	Provide attachment(s) Data Backup /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 buildings	Policies should cover: • **Data Protection** Clear details setting out how data is kept safe, the limits to access data, roles and responsibilities, guidance for handling data • **Information Security** Premises security, access to ICT systems, ICT security, **Records Management** What records are kept, who can access them, how to record, safe data transfer • **Subject Access Request Procedure** Staff and user awareness, process, roles and responsibilities defined. Arrangements for Sub-Processors • **Data Disposal** Procedure/policy retention period, safe disposal e.g. shredding or secure waste bins, electronic records, end of contract process.	Scored: [1] [2] [3] [4] [5]

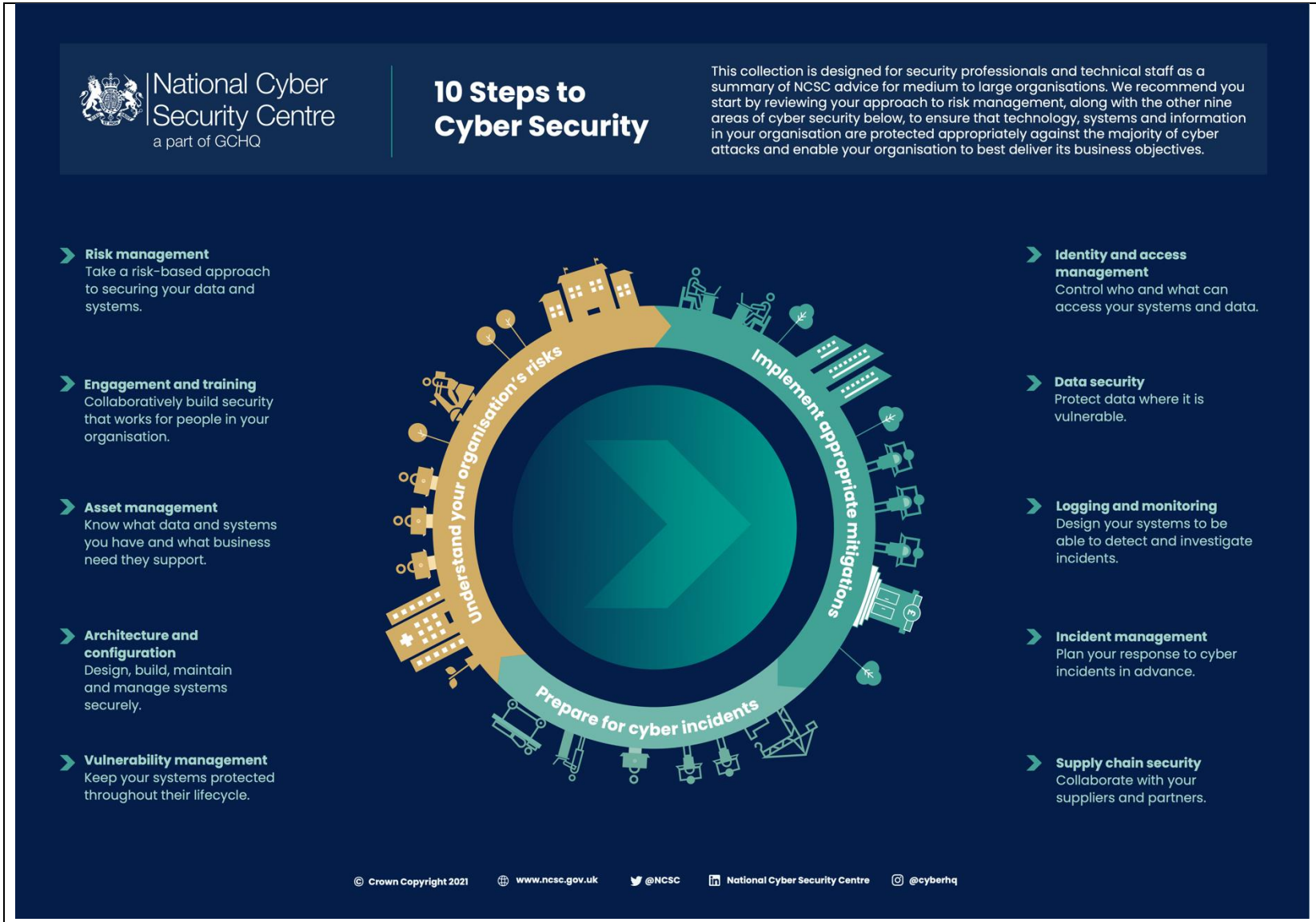
No	Question	Response	Guidance	Score
2	Do you assess data / privacy risks? How?	[Yes] or [No] Provide details and/or attachment(s)	Use of privacy impact assessment for new data processing / willing to use template for this contract	[Pass]/[Fail] Scored: [1] [2] [3] [4] [5]
3	Do you keep a central record of data processing activities?	[Yes] or [No] Provide details and/or attachment(s)	• The record should set out data processed, purpose, condition for processing, responsible person, any ICT system, retention period • If more than one, 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)	[Pass]/[Fail] Scored: [1] [2] [3] [4] [5]
4	What are your policies and procedures for dealing with security incidents / data breaches?	Provide details and/or attachment(s)	Clear process: who to report to, who will investigate, evaluation of the incident and resolution, e.g. lost file, computer virus	Scored: [1] [2] [3] [4] [5]

No	Question	Response	Guidance	Score
5	**Staff Training and Awareness** Does everyone in your organisation receive appropriate training and awareness briefings on data protection and information security including? • The Board • Senior management • Specialist Security staff • IT staff • All other staff Please describe the nature of the training given, when it is given and who is responsible for carrying it out.	[Yes] or [No] Provide details and/or attachment(s)		Scored: [1] [2] [3] [4] [5]

No	Question	Response	Guidance	Score
6 (See also 11)	**Organisational and Technical Measures to protect Personal Data** 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.	[Yes] or [No] Provide details and/or attachment(s) Alternatively: Provide a summary of your '10 Steps' approach in Section No 11 below.	ICT security controls are in place to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access **Accreditation / Certification is desirable:** e.g. Cyber Essentials, Cyber Essential Plus, ISO27001, IASME Governance. Alternatively: If your organisation is not accredited or certified, demonstrate your compliance with the National Cyber Centre (NCSC)'s '10 Steps to Cyber Security' at Section No 11 below.	[Pass]/[Fail]
7	**Location of Data** Confirmation of where electronic data is (to be) held [in house or off-site and in which country or territory]	[onsite] or [offsite] Also specify location(s)		Information only

No	Question	Response	Guidance	Score
8	**Backups** Do you regularly back-up data?	[Yes] or [No] Provide details and/or attachment(s)	Systems back up/ business continuity appropriate to type of data • Paper records • Cloud storage	[Pass]/[Fail] and Scored: [1] [2] [3] [4] [5]
9	**Data Transfers** Do you transfer personal data? If so, explain how data is transferred? Please confirm that all personal data processing occurs within the EEA or countries/territories about which the UK has made a positive adequacy decision.	[Yes] or [No] Provide details and/or attachment(s)	 e.g. Encrypted email, tracked post for special category data e.g. where are your tools such as SurveyMonkey / Mail Chimp and Google Analytics hosted	[Pass]/[Fail] (if applicable) and Scored: [1] [2] [3] [4] [5]

No	Question	Response	Guidance	Score
10	**Monitoring Mechanisms for Compliance with the General Data Protection Regulation is assessed at least annually.** For example, • Information Security audits • Records Management audit • Business Continuity and Disaster recovery plan tested • Formal accreditation or certification e.g. NHS Data Security & Protection Toolkit, IASME Governance	[Yes] or [No] Provide review plans and other details and/or attachment(s)	You should have plans in place to conduct audits of the information or processes relating to your compliance with Data Protection Legislation	[Pass]/[Fail] and Scored: [1] [2] [3] [4] [5]
11 (See also 6)	The 10 areas (Steps) to be used as headings under which to provide your response are: 1. Risk management 2. Engagement and training 3. Asset management 4. Architecture and configuration 5. Vulnerability management 6. Identity and access management 7. Data security 8. Logging and monitoring 9. Incident management 10. Supply chain security		This section only needs to be completed if your organisation does not have an appropriate accreditation or certification - See Section No 6 above. See the NCSC *infographic* below and for more detailed guidance behind the '10 Steps', refer to the NCSC website at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security	[Pass]/[Fail]


National Cyber Security Centre
a part of GCHQ
10 Steps to Cyber Security
This collection is designed for security professionals and technical staff as a summary of NCSC advice for medium to large organisations. We recommend you start by reviewing your approach to risk management, along with the other nine areas of cyber security below, to ensure that technology, systems and information in your organisation are protected appropriately against the majority of cyber attacks and enable your organisation to best deliver its business objectives.
Risk management
Take a risk-based approach to securing your data and systems.
Engagement and training
Collaboratively build security that works for people in your organisation.
Asset management
Know what data and systems you have and what business need they support.
Architecture and configuration
Design, build, maintain and manage systems securely.
Vulnerability management
Keep your systems protected throughout their lifecycle.
Understand your organisation's risks
Implement appropriate mitigations
Prepare for cyber incidents
Identity and access management
Control who and what can access your systems and data.
Data security
Protect data where it is vulnerable.
Logging and monitoring
Design your systems to be able to detect and investigate incidents.
Incident management
Plan your response to cyber incidents in advance.
Supply chain security
Collaborate with your suppliers and partners.
© Crown Copyright 2021
www.ncsc.gov.uk
@NCSC
National Cyber Security Centre
@cyberhq