Appendix 12a

Risk Assessment Process for Security of Data

SMA UK has a comprehensive and detailed approach towards data security and of risk assessment.

When considering a new project each aspect of data security should be considered and risk assessment of individuals data security made before a project is implemented. This should be recorded on the Data Protection Impact Assessment proforma. Any medium and high-risk element should be considered, and every effort should be made to lower or eliminate these. There is a place on the form to record these.

The risk assessment approach

1. Firstly, think about the threat events which could impact the confidentiality, accuracy, or availability of the data you are collecting, processing or storing.

2. Next assign a numerical value as listed below.

Highly Probable	5	The event will certainly occur
Probable	4	The event is likely to occur
Possible	3	The event could occur
Unlikely	2	Little chance of the event happening
Highly unlikely	1	Almost no chance of it occurring

3. Then consider the impact of the event

Disclosure of personal details, such as name, address, telephone number, emails, date of birth, gender, medical data, bank details, conversations and any additional data, which could result in a large number data subjects suffering harm, anxiety or identity theft as a direct result of disclosure.	5
Disclosure of personal details, such as name, address, telephone number, emails, date of birth, gender, medical data, bank details, conversations and any additional data, which could result in small number data subjects suffering harm, anxiety or identity theft as a direct result of disclosure.	4
Disclosure of some personal details, such as name, address, emails, telephone number, date of birth, undefined medical data or personal contact of some data subjects	3
Disclosure of name, address, emails, telephone number, date of birth, of some data subjects	2
Disclosure of no more than two personal details, from name, address, emails, telephone number or date of birth of data subjects	1

4. Multiply the Likelihood value by the Impact value to determine a risk score

5. This score will provide you with a ranking for each event. Place the numerical value in the appropriate column of the Data Protection Impact Assessment

6. This allow you to consider what controls are in place to minimise the risk, what further controls need to be considered or if the risk is too high.

Examples

A. It has been decided to buy password protected and encrypted data sticks for some members of staff. Staff have been trained in security measures of using the sticks and computers of site to reduce risk and have a lockable place at home to store stick. Sticks are locked away if kept in the office. Information is deleted after use on a fortnightly basis and tend to hold no more than 5 records in one time and contain no bank details.

Event	Likelihood	Impact	Result	Comment
Loss of data stick and data removed	2 – due to sticks being encrypted	3	2X3=6	Low Risk – Remind staff to clear data at all times and ensure, that care in taken to secure sticks. As the sticks are encrypted every effort has been made by the organisation to secure risk.