Appendix 10

Data Protection by Design and Default

In accordance with Article 25 of General Data and Protection Regulations, SMA UK ensures that all systems for data processing and storage are subject to assessment of Data Protection by Design and Default. When implementing a system for collecting, processing and storing data we take appropriate measures to protect personal data.

By Design

From the very beginning of the design stage or the moment that the means of data processing are decided upon, we design and implement appropriate technical and organisational measures to implement data protection principles, considering:

- The state of the art technologies available
- The effectiveness of implemented systems
- The cost of implementation
- Nature, scope, context and purposes of processing;
- The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing

We ensure that all systems for data processing and storage follow the 'Seven foundational principles of privacy by design' as detailed by 'The Information & Privacy Commissioner of Ontario (IPC) which has taken a leading role in developing the privacy by design and is recommended by the Information and Commissioners Office (ICO). For more details click **here.**

1. Proactive not reactive; preventative not remedial (Anticipates privacy invasive events)
2. Privacy as the default setting (Data is automatically protected by default)
3. Privacy embedded into design (Data protection is part of the design not bolted on)
4. Full functionality – positive-sum, not zero-sum (All legitimate interest is considered in the design, there are no trade-offs e.g. security vs privacy)
5. End-to-end security – full lifecycle protection (All data is securely retained and securely destroyed at the end of the process)
6. Visibility and transparency – keep it open (All processes are visible and transparent)
7. Respect for user privacy – keep it user-centric (That it is user friendly)

In addition, for any new Processing or when the there is a high risk to the rights and freedoms of the data subject, we carry out Data Protection Impact Assessments (DPIA's) using an internal proforma, which includes the assessment of and strategies used to mitigate risk. In the event of a significant change to data collection or storage or introduction of new technologies a more detailed DPIA will be implemented in line with ICO's Privacy Impact Code of Practice

By Default

All technical and organisational measures are taken to ensure that only personal data which are necessary for a specific purpose are processed. We attempt where possible to minimise the amount of data we process. To ensure this we always consider the following

- The amount of data collected
- The extent of processing required
- The storage period and accessibility.

The practical implementation of this is outlined in more detail in our Confidentiality and Data Protection Policy

Last reviewed Feb 2021