DATA PROTECTION PRINCIPLES

7 DATA PROTECTION PRINCIPLES

All processing of personal data must take place in accordance with the seven data protection principles under the GDPR (Article 5). Below is a description of the principles:

1. ACCURACY

Processing of personal data must be done with accuracy. The Controller is responsible for ensuring that any personal data that is incorrect, must be corrected or deleted.

2. LAWFULNESS, FAIRNESS AND TRANSPARENCY

All processing of personal data must be legal, correct and transparent and nothing shall be hidden from the data subjects regarding the processing of their personal data.

3. PURPOSE LIMITATION

The processing of personal data may only take place for specific purposes that are specifically stated and justified, for the time that is necessary for the purpose. It is not permitted to collect personal data without a certain specifically stated purpose.

4. DATA MINIMISATION

It is only permitted to process necessary, relevant and adequate personal data for the specific purpose in question.

5. INTEGRITY AND CONFIDENTIALITY

Personal data must be processed in a way that ensures appropriate security and must also be protected against damage, loss or unauthorized processing through technical and organizational security measures.

6. STORAGE LIMITATION

Personal data shall be deleted or anonymised when they are no longer necessary to process for the purposes for which they were collected. Erasure must take place from all storage locations where the data is stored.

7. ACCOUNTABILITY PRINCIPLE

It is not enough to simply claim compliance with the GDPR. The Controller must also be able to prove that he complies with the GDPR in practice and show how the regulations are complied with. For example, this can be done by establishing various GDPR agreements and internal routines regarding processing and logbooks to record completed erasures etc.