

THE DATA PROTECTION ACT 2018 PRINCIPLES

(SUMMARY)

The following principles must be applied to all processing of personal data:

1. The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair.
2. The second data protection principle is that:
 - (a) the law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and;
 - (b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.
3. The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. The fourth data protection principle is that:
 - (a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and;
 - (b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.
5. The fifth data protection principle is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.
6. The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).