GUIDELINE ON USAGE OF UNMANNED AIRCRAFT SYSTEMS (UAS) IN COMPLIANCE WITH DATA PROTECTION

UAS may be covered by the Data Protection Act when it processes personal data. For example, a UAS can have embedded technology such as a camera/microphone which offers the possibility to collect and record personal images/sound allowing operators to identify persons directly or indirectly.

UNMANNED AIRCRAFT SYSTEMS FOR PERSONAL USE

Individuals using UAS to process personal data for personal use must ensure that they do not infringe on the right to data protection and privacy of any other data subject.

UNMANNED AIRCRAFT SYSTEMS FOR PROFESSIONAL / COMMERCIAL USE

It is the responsibility of the **data controller** (i.e, the organisation which is using the UAS to process personal data) to abide by all the provisions of the Data Protection Act, including to:

1) Notify people about the operation of the UAS, the purposes for which it is being used and the identity of the operator.
2) Obtain the consent of data subjects for processing their personal data unless the exceptions under section 24(2) apply.
3) Be able to provide strong justification for the use and identify all personal data that may be captured.
4) Perform a robust Privacy Impact Assessment.

   Note: A Privacy Impact Assessment is a self-assessment tool to be used by organisations to assess their compliance with data protection. The guideline 'Vol. 6 - Guidelines on Privacy Impact Assessments' available on http://dataprotection.govmu.org explains how organisations can carry out the self assessment.

5) Ensure that it has registered as data controller with the Data Protection Office for all personal data processed.
6) Ensure that it is necessary and proportionate with respect to the purpose being used.
7) Ensure that any personal data which has been collected is stored securely, for example by using encryption or another appropriate method of restricting access to the information.
8) Ensure that personal data is retained for the minimum time necessary for its purpose and disposed of appropriately when no longer required.
9) Incorporate privacy by design methods to reduce the risk of collateral intrusion. For example, a data controller can procure a device that has restricted vision so that its focus is only in one place.
10) Prevent any unlawful disclosure of personal data.