DRONEMARK BEST PRACTICES

Dronemark observes the following best practices for privacy, transparency, and accountability.

1. Inform Others of Your Use of UAS

1(a) Where practicable, UAS operators should make a reasonable effort to provide prior notice to individuals of the general timeframe and area that they may anticipate a UAS intentionally collecting covered data.

1(b) When a UAS operator anticipates that UAS use may result in collection of covered data, the operator should provide a privacy policy for such data appropriate to the size and complexity of the operator, or incorporate such a policy into an existing privacy policy. The privacy policy should be in place no later than the time of collection and made publicly available. The policy should include, as practicable:

- the purposes for which UAS will collect covered data
- the kinds of covered data UAS will collect
- information regarding any data retention and deidentification practices
- examples of the types of any entities with whom covered data will be shared
- information on how to submit privacy and security complaints or concerns
- information describing practices in responding to law enforcement requests

Material changes to the above should be incorporated into the privacy policy.

2. Show Care When Operating UAS or Collecting and Storing Covered Data

2(a) In the absence of a compelling need to do otherwise, or consent of the data subjects, UAS operators should avoid using UAS for the specific purpose of intentionally collecting covered data where the operator knows the data subject has a reasonable expectation of privacy.

2(b) In the absence of a compelling need to do otherwise, or consent of the data subjects, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of covered data about individuals.

2(c) Where it will not impede the purpose for which the UAS is used or conflict with FAA guidelines, UAS operators should make a reasonable effort to minimize UAS operations over or within private property without consent of the property owner or without appropriate legal authority.

2(d) UAS operators should make a reasonable effort to avoid knowingly retaining covered data longer than reasonably necessary to fulfill a purpose as outlined in 1(b). With the consent of the data subject, or in exceptional circumstances (such as legal disputes or safety incidents), such data may be held for a longer period.

2(e) UAS operators should establish a process, appropriate to the size and complexity of the operator, for receiving privacy or security concerns, including requests to delete, deidentify, or obfuscate the data subject's covered data. Commercial operators should make this process easily accessible to the public, such as by placing points of contact on a company website.

3. Limit the Use and Sharing of Covered Data

3(a) UAS operators should not use covered data for the following purposes without consent: employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility other than when expressly permitted by and subject to the requirements of a sector-specific regulatory framework.

3(b) UAS operators should make a reasonable effort to avoid using or sharing covered data for any purpose that is not included in the privacy policy covering UAS data.

3(c) If publicly disclosing covered data is not necessary to fulfill the purpose for which the UAS is used, UAS operators should avoid knowingly publicly disclosing data collected via UAS until the operator has undertaken a reasonable effort to obfuscate or de-identify covered data —unless the data subjects provide consent to the disclosure.

3(d) UAS operators should make a reasonable effort to avoid using or sharing covered data for marketing purposes unless the data subject provides consent to the use or disclosure. There is no restriction on the use or sharing of aggregated covered data as an input (e.g., statistical information) for broader marketing campaigns.

4. Secure Covered Data

4(a) UAS operators should take measures to manage security risks of covered data by implementing a program that contains reasonable administrative, technical, and physical safeguards appropriate to the operator's size and complexity, the nature and scope of its activities, and the sensitivity of the covered data.

For example, UAS operators engaging in commercial activity should consider taking the following actions to secure covered data:

- Having a written security policy with respect to the collection, use, storage, and dissemination of covered data appropriate to the size and complexity of the operator and the sensitivity of the data collected and retained.
- Making a reasonable effort to regularly monitor systems for breach and data security risks.
- Making a reasonable effort to provide security training to employees with access to covered data.
- Making a reasonable effort to permit only authorized individuals to access covered data.

5. Monitor and Comply with Evolving Federal, State, and Local UAS Laws

5(a) UAS operators should ensure compliance with evolving applicable laws and regulations and UAS operators' own privacy and security policies through appropriate internal processes.