Guidance on the Use of Drones

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Drones and Data Protection

Drones (common name for Unmanned Aerial Systems (UAS)) are a broad category of aircraft of various sizes which are remotely piloted without humans on board, equipped with technology for collecting images, videos, sounds and/or other information (data collection system) and transmitting them to smart devices (for example, to cloud storage). Similar to Body Worn Cameras (BWC) (see: Guidance on Body Worn Cameras) drones can effectively turn into a mobile surveillance system and are highly likely to capture the personal data of passers-by (data subjects) (see: Data Protection: The Basics). These guidelines have been developed for drone operators for purposes other than public law-related purposes (see: Law Enforcement Directive) and also to answer queries from the perspective of data subjects. Other drones aviation particulars such as security, safety and certification requirements remain outside the scope of these guidelines (see: Irish Aviation Authority www.iaa.ie).

Drone Operators as Data Controllers

Regardless of the nature (professional or recreational) of your activity, under EU law regulating unmanned aircraft[1] the collection of information related to an **identifiable person** through the operation of a data collection system mounted on a drone potentially constitutes personal data processing (see: Data Protection: The Basics). If you qualify as **data controller**, because you determine the purposes and means of the data processing activity (see: Data Protection: The Basics), you are obliged to comply (and be able to demonstrate that you are compliant) with all applicable data protection law (see: Guidance on the Principles of Data Protection) unless your activity with the drone can be considered to be purely household or personal activity.

For example, if a drone is **equipped with a camera**, and you operate that camera to record video/images at such height that you may identify someone, even with the assistance of other tools such as zooming, you are likely to be processing personal data and also to qualify as a "data controller" because you have decided to use the drone to capture images of someone.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0947

Lawfulness of Processing

As with any processing of personal data, the recording of identifiable images of persons must have a legal basis under the data protection legislative frameworks. The consent of an individual to the processing of his or her personal data can provide a legal basis to process data. However, this is unlikely to apply to most uses of drones as it will be difficult to obtain the freely given consent of everyone likely to be recorded.

Often, drones can be used by the owners and occupiers of premises in pursuit of their legitimate interests in viewing their land. Such legitimate interests may provide a legal basis for the processing of personal data, provided that the interests of the data controller are balanced with, and not overridden by, those of the individuals whose personal data are being processed.

When relying on legitimate interests as a legal basis to utilise drones, the data controller should be able to demonstrate that:

- ☑ It is genuinely in their interests to do so
- ☑ That it is necessary to achieve their identified purpose(s)
- ☑ That it does not have a disproportionate impact on the individuals whose personal data will be processed, by way of having a minimal impact on their privacy or by virtue of the nature of the processing or the safeguards introduced.

An example of such a safeguard is automated blurring software which automatically blurs faces, bodies and license plates on images and videos.

Household or Personal Activity

If you use a drone in the context of a professional or commercial activity (for example, if you are a professional photographer or are conducting farmland surveys by aerial mapping in the course of your farming activity), such use will not fall under the definition of "household or personal activity".

On the other hand, **recreational activity** may qualify as household or personal activity and fall outside the scope of data protection law depending on the **circumstances of the case**, in particular on the use of the data after collection and on the manner of collection.

For example, if your hobby is photography and you want to **try your new drone** in a public park, the drone's camera may accidentally record other people. Whilst your activity will not qualify as "household activity", it does not amount to surveillance activity either, and **may be** qualified as purely personal activity if you do not publish your recordings to an unrestricted audience. There is nothing under the GDPR

prohibiting people from taking photos in a public place. Provided you are not harassing anyone, taking photographs of people in public is generally allowed. However, whether you can publish a photograph to a broad-based audience is a different question. In other words, taking a photo in public is generally fine; it's what you do with that photo that can potentially become a data protection issue.

If, on the other hand, you set up and fly your drone for the purposes of **surveillance over a vast garden** of yours, this activity may not be considered a "household or personal activity" if the camera mounted onto the drone is able to record images of the surrounding private property/public space. For example, if there is no system in place for the drone to fly at such height that it only records images of your own property. This situation would be similar to that of CCTV installed in private premises (see: Guidance on the Use of CCTV).

If your activity with drones does qualify as household or personal activity, the Data Protection Commission (DPC) nonetheless recommends that you apply a common sense approach, **and keep in mind that other legal requirements may apply to your activity.** You should always try to avoid encroaching on the personal space and the privacy of others by recording their images or further processing same.

Relevant Data Protection Obligations

As data controller, **before you fly a drone**, you must ensure that you comply – and be able to demonstrate to the DPC at any time that you are compliant (see: Accountability Obligation) – with all applicable data protection obligations (see: Know Your Obligations).

You may need to assess the data protection issues of your activity by conducting a data protection impact assessment (see: Data Protection Impact Assessment) and prepare a data privacy policy.

Some **key issues for data controllers who are drones operators** are specifically considered below:

- Comply with all applicable laws, not only data protection (for example, tort law on trespassing or aviation law), in order for your data processing activities to be **lawful**;
- Define the **purposes** for which you collect personal data with your drone, and eventually further process them for the same or compatible purposes, including disclosing data to third parties (see: Legal Bases for Processing).

For example, if the purpose of recording images with the drone is the **settlement of possible personal injury claims**, further disclosure to a lawyer may be permissible, as commencement of **legal proceedings** is compatible with the initial purpose, whereas online disclosure of the images to an unlimited audience since it also contained a funny scene of the incident which could go viral would not be compatible with the settlement purpose.

- Rely on a **legitimate basis** in order to carry on your data processing activities, which depends on the circumstances of your case (see: Legal Bases for Processing).

For example, consent could be a legitimate basis for the **recording of a sport training session** of a team by a drone equipped with camera, as it may be feasible to collect free, informed and unambiguous consent from the team members in advance of the training, whereas it would be difficult to collect valid consent for the **surveillance of farmland** by drones from persons such as trespassers. Legitimate interest of the landowner in protecting goods and property could be relied upon instead (see: Legal Bases for Processing).

- Provide data subjects with the **information** required, and in the form provided, by data protection law (see: Providing Transparent Information) as soon as you collect their personal data (at the moment of recording information with the drone), so that they will be able to exercise their rights (see: Your Rights under GDPR). The specific measures will depend on the context and environment in which the data is collected.

For example, if drones are used in public areas where the recording perimeter cannot be easily defined (for example in the case of a stadium, or at the entrance to farmland or other private property), **privacy notices may not be enough**, and you may adopt a layered approach:

a) Have signage outside the venue or at certain perimeter points;
b) Signal that the drone in operation is recording using sounds/flashing lights;
c) Identify yourself as the drone operator by wearing highly visible clothing and be ready to provide the information required by QR codes link to a website containing a privacy notice.

- Collect and use the personal data only insofar it is strictly necessary in accordance with your purposes ("**data minimisation**"). Set up the data collection system of your drone and the data storage systems in a way that, by default,

avoids unnecessary collection and further processing for example by anonymising data (see: Anonymisation and Pseudonymisation).

For example, the recording camera **automatically recognises and blurs** images of physical persons if you are collecting data only to assess the existing status of the grass on farmland.

Buying a Drone

As data controller, it is your responsibility to ensure that the drone system you will be using is compliant with **privacy by design and by default** (see: Data protection by Design and by Default). When buying your equipment, you must check whether the device has been produced with data protection obligations in mind.

For example, in order to comply with data minimisation, data collection systems mounted on drones should be capable of being **switched on and off** when appropriate and their **visual angle limited** in accordance with your purposes (i.e. you do not need a 360 angle if you fly your drone for the purposes of assessing specific roof damage after a storm). In order to comply with the transparency principle, the drone should have adequate signalling, such as, for example, **lights or buzzers.**

It is your responsibility to ensure that appropriate technical and organisational measures are in place for the **security** of processing (see: Guidance on Data Security), bearing in mind that in case of failure of any of such measures you may have breached the obligation to process personal data according to the principle of integrity and confidentiality, and you may be obliged to report a personal data breach (see: Personal Data Breach Notifications). Pay particular attention to the technological security features embedded in the drone system for collection and storage of data.

For example, check whether the video footage is stored on the device itself, on a portable storage medium (such as memory stick), or on a cloud storage service and take steps to mitigate any additional risk of loss or theft of personal data, such as encrypting data before they are transferred from the device to the cloud storage. You should remain vigilant about 'eavesdropping', remote control interference and other forms of attack when remotely operating drones.

Use of Third-Party Services

When setting up your drone, you may use third-party services such as cloud storage in order to securely and easily store the data collected with your drone. Providers of these services may be qualified as **data processors** when processing personal data on your behalf. As data controller, you would bear the main responsibilities under data protection law (see: Data Protection: The Basics) and your relations with processors must be governed by a **written contract** (see: Guide to Controller-Processor Contracts) outlining the responsibilities of processors for each operation of the drone collection and storage system. In the case of **joint controllers** (for example, when you collect data and share same with an advertising agency or a client) specific obligations such as drafting a document outlining the respective responsibilities may apply (see: Controller and Processor).

For example, it may be necessary that you carefully consider whether any such third party providing services to you is **located outside the EEA** (EU Member States, Iceland, Liechtenstein and Norway). In the absence of a decision from the European Commission on the adequacy of the data protection legislation in force in any country outside the EEA, it is your responsibility to ensure that transfer of personal data to these countries is lawful (see: Transfers of Personal Data).

Suspicious Drone Activity

To raise a concern with the DPC related to your data protection rights, you must provide the **details of the data controller** (which you should try to **contact yourself first** wherever possible and appropriate). The DPC will be unable to progress a complaint unless the identity of the controller is provided and there is evidence that the processing of your personal data took place.

Where the DPC identifies infringements of data protection legislation in any sector or scenario, it has powers to sanction, including applying administrative fines (for more information on how to exercise your rights, please visit the Raising a concern).

If you do not know the identity of the drone operator, you may refer the matter to your local Garda station, as well as in any other event of concern which is not related with data protection (see: www.garda.ie/en/contact-us/).

Use of Drones in the DPC Decision on Limerick City and County Council[2]

In 2021, the DPC concluded an own-volition inquiry into the surveillance activities of Limerick City and County Council. Authorised Officers from the Special Investigations Unit of the DPC were authorised in June 2018 to conduct a connected series of investigations under sections 110 and 123 of the 2018 Act into a broad range of issues pertaining to surveillance technologies deployed by state authorities, in particular, the various local authorities and An Garda Síochána for law enforcement purposes.

As part of this decision, the DPC inquired into Limerick City and County Council's use of drones. Drones were in use by the Council for waste enforcement purposes. It was stated by the Council that it did not set out to use a drone to capture images of persons. However, the Council submitted that, in the event an image of a person was caught in the act of dumping waste, this image would be used for the purpose of investigating the offence. Separately, the Water Monitoring Section of the Council used drones to survey the waterways in the context of its law enforcement powers under the Water Pollution Acts. The Council submitted it may use any images it captured of suspected polluters for investigation and prosecution purposes.

The decision therefore found that the Council processed personal data in its use of drones. Despite this, the Council had made no efforts to provide the information required by section 90 of the 2018 Act at the time the personal data was processed by the drones, or after the processing occurred to the general public. The decision found this information could have been supplied on the Council's website. Furthermore, the Council had no data protection policy governing its use of drones until 8 November 2018. The decision found that the Council was using drones for the detection of crime and that in failing to carry out a DPIA before doing so had not fulfilled section 82(1) of the 2018 Act.

The decision ordered the Council to bring its processing by means of drones used primarily for the purposes of law enforcement into compliance with section 90(1) of the 2018 Act by ensuring that all data subjects are provided with all the information required by section 90 of the 2018 Act. The Council was required to make the information required by section 90 easily accessible to data subjects by placing, in an easily accessible location of the website, a detailed Drones Policy which gives information on the locations where drones will be operated and the relevant information required by section 90.

[2] https://www.dataprotection.ie/sites/default/files/uploads/2022-01/REDACTED_091221_Final%20DecisionLimerick_03-SIU-2018%20PDF%20FINAL.pdf