agencia española protección datos

Drones and Data Protection

DRONES AND DATA PROTECTION

It cannot be denied the use of drones among the general public has grown exponentially in recent times.

The default configuration of any drone includes at least one GPS and a video camera and from there on all kinds of data acquisition and processing devices such as thermal imaging cameras, night vision cameras, 3D scanners, WiFi and/or Bluetooth devices, mobile device detection systems, etc.

The right to data protection is a fundamental right that guarantees any person's capacity to decide on their own personal information. The use of drones such as those mentioned above may impact on a person's right to data protection and, therefore, may constitute a violation of their rights and freedoms.

Taking into account the definition of personal data as "any information relating to an identified or identifiable natural person", operators of drones who register and/or process the images, video, sound, biometric data, geolocation or telecommunication data related to an identified or identifiable person are subject to the General Data Protection Regulation (GDPR) and Organic Law 3/2018, of 5 December on the Protection of Personal Data and Guaranteeing Digital Rights (LOPDGDD as per the Spanish).

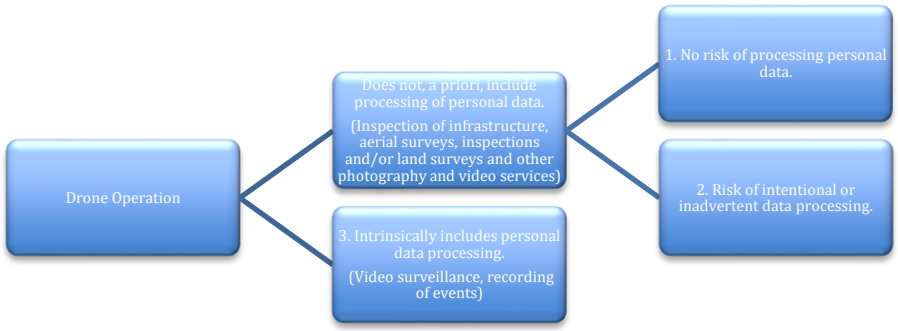
One must take into account that on occasions an item of data can directly identify a person, such as for example their photograph, but on other occasions the identification is not direct and requires additional processing, such as geolocation information or by enriching it with other additional data such as, for example, the internet and, even though, a priori, the person may be identifiable, the final result would mean that the identification is possible thanks to crossed information from different sources. Whether the data collected by drones unequivocally identifies a person, or if such may be the case subsequently, data protection regulation applies.

The specific regulation for the use or airspace applies in parallel with personal data protection regulation in accordance with the general obligations set out in Article 26 of Royal Decree 1036/2017, of 15 December, regulating the civil use of remote controlled aircraft, establishing the obligation to adopt the necessary measures to guarantee compliance with the provisions on data protection and the protection of privacy. Therefore, in addition to the provisions established in air-space legislation mentioned above, it must be borne in mind that the GDPR and LOPDGDD apply fully to the processing of personal data through the use of a drone, regardless whether the operation of the drone takes place in the professional or recreational sphere.

TYPE OF OPERATIONS DEPENDING ON DATA PROCESSING

The main applications of drones are video surveillance, inspection of infrastructure, topographic surveys, agricultural inspections and/or precision agricultural management and other photograph and video services (for cinema and tv, property services, etc.), internet access services, etc. However, the availability of multiple devices for the acquisition of data and increasingly more advanced platforms would suggest the inevitable emergence of numerous applications.

From a perspective focussing strictly on data protection, drone operations can be classified into two main categories depending on the purpose of the operation. On the one hand there are those for which the purpose of the operation itself involves personal data processing, such as the case of video surveillance or surveillance of persons using any other type of sensor (such as mobile device surveillance) and, on the other hand, there are those operations whose purpose does not, a priori, include the processing of personal data, such as the inspection of infrastructure, topographic surveys, filed inspections and other photography and video services that may, at a given time, impact on people's right to personal data or privacy.



1. OPERATIONS THAT DO NOT INCLUDE PERSONAL DATA PROCESSING

These types of operations are less frequent and they may include operations with drones with very basic configurations that may or may not include GPS positioning for flight assistance but lack or make no use of devices for the capture of images, sound or any other types of personal data or information.

This category may also include operations within the recreational ambit with drones equipped with GPS and cameras, but in which the use of the images captured is restricted to domestic use or do not permit the identification of a person under any circumstances.

In these cases:

- Before sharing internet images or videos captured with a drone, it is necessary to ensure that they do not contain images or data relating to persons, vehicles, residences or other objects that may lead to the identification of data subjects and in the affirmative case, anonymise them using blurring techniques or similar.
  Examples:
  - A very low resolution camera is used, that does not capture a defined image of a person's face in such a way that it allows them to be identified but the image of the person appears in their residence in such a manner that the location where they appear could allow their identification.
  - The image does not allow for the identification of the person driving a vehicle but the registration of the vehicle would make their identification possible.

  In both cases it would be necessary to carry out post-processing or editing of the images for the purpose of preventing the identification of persons using image blurring techniques.

2. OPERATIONS WITH A RISK OF COLLATERAL OR INADVERTENT PERSONAL DATA PROCESSING

In operations such as inspection of infrastructure, topographical surveys, inspections and/or agricultural processing and other photography and video services (for cinema, TV, advertising, etc.), even where it is not the purpose of the operation, there is a risk of the capture of personal data unintentionally or inadvertently. This may occur because the capture of certain images of persons in the background or the capture of other types of

information (nearby residences, recreational areas, vehicles, etc.) or because specific characteristics of the operation, e.g. operations beyond the visual scope of the pilot, is inevitable.

In such cases it is necessary to comply with the following recommendations:

- Minimise the presence of persons and objects that allow for their identification (for example, bathers, vehicle registrations, etc.) in the area of the operation. This can be done by, for example, performing flights, where possible, at times where there are not large concentrations of people or when access to the flight zone is restricted.
- Minimise the capture of images to those absolutely necessary, reducing the possibilities of persons appearing inadvertently in the images and considering the possibility of not capturing the full flight but those moments necessary. This recommendation can be extended to any form of data collection.
- Promote and apply privacy features from design such as, for example, adjusting the resolution of the image to the minimum necessary to execute the purpose of the processing, reduce the granularity of geolocation for the same purpose, apply techniques for the anonymization of images (automatically during the capture or procedures to do so immediately subsequently) or mechanisms to initiate and stop the capture of data at any time during the operation, to implement secure communication protocols that prevent third party access to the captured data transfers and even control of the device itself or to include mechanisms that allow for the encryption of the data captured and stored on the drone itself.
- In areas where there will inevitably be people, complete the capture of images in a manner that persons cannot be identified, for example by capturing images only at a sufficient distance to ensure that their identification is not possible.
- Prevent the processing of another type of personal data such as, for example, the indiscriminate capture of mobile device identifiers.
- Prevent the storage of unnecessary information relating to persons. For example, if the purpose of the images is a topographical survey of a coastal area, it would not make sense to store images allowing bathers located in that area to be identified.

3. OPERATIONS THAT DO NOT INCLUDE PERSONAL DATA PROCESSING

Such is the case of video surveillance, recording of events and any other application for which the purpose of the operation intrinsically involves the processing of personal data.

In these operations, the GDPR and the LOPDGDD both apply, along with the provisions set out in the Spanish Data Protection Agency's Guide to the Use of Video Cameras for Security and other Purposes (in Spanish), which establishes the limits to video surveillance through camera or video camera systems or the monitoring of mobile device identifiers, in particular so that the installation of video cameras in public places for security purposes, both fixed and mobile, is exclusively the competency of the state security forces.

Moreover, it is necessary to observe the following additional recommendations:

- On the role of the operator:

- If the processing is performed by a third party who takes decisions relating to the purpose of the image (for example, the purpose of video surveillance), this third party will be the data controller. The drone operator will be considered a data processor and it must be ensured that their relationship with the data controller is governed by a legal contract or deed which links it to the data controller and that it only acts in accordance with the instructions of the data controller. In terms of data protection, the data controller is the person who decides as to the purpose of the processing while the data processor is the party who processes the data following the guidelines and instructions set out in a contractual relationship between the two.

  For more information on preparing a data processing contract, see the Guidelines for preparing contracts between data controllers and data processors (in Spanish).
- If the operator is acting as data controller: They must determine the most appropriate legal basis upon which to carry out the processing (consent, contract, legal obligation, legitimate interest, etc.). In general, they must meet the obligations set out in the GDPR.

- Choose the on-board technology most appropriate to the purpose pursued with the operation and adopt all of the appropriate default security measures, avoiding the subsequent gathering and processing of unnecessary data.
- Implement mechanisms to exercise the right to information in relation to the processing of personal data carried out, taking into account the singular nature of drones but without forgetting that the information provided must be clear and transparent and can be provided electronically.

  Therefore, the most appropriate method of informing those who will be affected by the processing of the data must be found: informing by signs or informative sheets, social media publications, newspapers, leaflets, posters, etc. stating the identity of the data processor and the purpose of same and those affected must be provided with clear and specific indications as to the exercise of their rights.

  For more information, please see the Guide to compliance with the duty to inform (in Spanish).
- Take the appropriate technical and organisational measures to guarantee a level of security appropriate for the risks to the rights and freedoms of people, in particular to prevent any unauthorised processing during the transfer phase of the data gathered.
- Remove or anonymise unnecessary personal information as soon as possible after gathering,
- Include options that respect privacy and predetermined functions as part of a privacy-by-design focus.
- Ensure that drones are as visible and identifiable as possible, with characteristics associated with the data controller, making the operator also visible and identifiable as controller of the drone. In this sense, where applicable, the identification and registration requirements referred to in Articles 8, 9 and 10 of Royal Decree 1036/2017 will be taken into account.

4. STEPS TO BE TAKEN PRIOR TO USE OF A DRONE

Where personal data protection regulation applies (see questions at the end of this text on the exception for personal and domestic processing) the following actions steps must be taken:

4.1. Check that national legislation allows for use of drones and, if necessary, request the authorisation of the aviation authorities. Where the operation of a drone violates the applicable national aviation legislation or any other which should be adhered to, it shall be considered that the capture of data and processing of same performed during aviation operations does not comply with the principle of legality contained in the GDPR, and will therefore be subject to the sanction regime on data protection (without prejudice to the fact that it may be subject to the sanction regime for aviation or other additionally applicable regimes).

4.2. When defining the campaign or service to be executed through drones and prior to the start of the operation in which it is intended to process personal data, the need to carry out an assessment of the risks involved in the processing for the rights and freedoms involved must be analysed. In the event that the processing is within the circumstances established in the GDPR or the list of cases established by the GDPR or the list of compulsory processing established by the AEPD, it will be necessary to complete a data protection impact assessment (DPIA) with the degree of detail required in the GDPR. If there is no explicit obligation to complete a DPIA, completing one will always be considered a good practice on the part of the data controller. This is completed taking into account the purpose of the operations, the type of drones and the detection technologies used. The impact assessment is carried out for each type of operation, even though it is not necessary to carry out an assessment each time a certain type of operation is performed. Finally, if necessary, the provisions of Article 36 of the GDPR in relation to the competent data protection authority should be consulted in advance.

4.3. If the needs analysis reaches the conclusion that is not necessary to complete an impact assessment, but there is a possibility that the operation encompasses potential risks for personal data protection, a risk analysis must be carried out for the purpose of adopting the necessary guarantees to, insofar as possible, mitigate those risks and their potential consequences for people's rights and freedoms. See the Spanish Data Protection Agency's Guide to risk analysis (in Spanish).

4.4. If images are captured for personal use, it is necessary to consider that they should not be published on the internet in such a way that they are accessible to an indeterminate number of people where it is possible to identify individuals or where private spaces are shown, for example, residences, garden, terraces, etc. One must take into account that even in those cases of personal or domestic processing which is not subject to data protection regulation, the information captured by the drone may violate the right to honour, personal and family privacy and people's image.

4.5. Assess, in advance, the objectives of the operation ensuring the physical security of the flight and comply with aviation legislation.

5. FAQS

Question 1: I have been contracted by a client to promote their hotel. I've made a photo report where guests appear in the spa, pool and sports facility areas. Can my client publish it on their website? Can I publish it on YouTube to promote my services as a photo reporter?

Answer: In this case your client is responsible for processing the images captured because they are the ones who decide upon the purpose of same. To publish images of their guests on their hotel website they would require the express consent of those guests. The absence of that consent could mean an infraction

of the GDPR. Moreover, the images of people, for example, in spa or swimming pool areas may affect their right to honour, privacy and one's own image, in addition to constituting a greater risk in relation to data protection.

If images of hotel guests are published on YouTube or on any publicly accessed website to promote services, you will be taking a decision on the purpose of said images and this will mean you are considered the data controller and, like the hotel you are working for, you will require the express consent of all guests whose images you are about to publish or mask or pixelate faces to prevent the identification of those persons.

In this case, it is recommended that images are captured from a distance or with a resolution that prevents the identification of the persons.

Question 2: I'm a drone operator and I have been contracted for the inspection of public roads. The drone uses a camera and GPS device to geo-reference the photographs taken when we detect an imperfection in the surface of a road. On some occasions we capture images of the registration plates of vehicles or even their occupants. It is our understanding that because we have not processed these images, data protection regulation does not apply.

Response: the capture of images of persons or registrations of vehicles and their recording and storage necessarily involves a processing of personal data and data protection regulation is applicable.

To do so, it would first be recommendable to choose a time in which less traffic exists for the purpose of minimizing the recording of images of people or vehicle registrations. If ultimately it is not possible to prevent the capture of images of persons or vehicle registrations, a post-editing process of images should be carried out to remove any data that allows for the identification of the persons

Question 3: I use a drone for video surveillance of a property. Where can I install a 'video surveillance in operation' sign?

Answer: Where a drone carries out functions of image capturing for the purposes of video surveillance, the GDPR applies and this involves, among other things, the need to comply with the duty to provide information set out in Article 13, the maintenance of a processing log and the adoption security measures based on the risk analysis performed.

The duty to inform regarding the processing of personal data in a processing activity for security purposes should be fulfilled by installing signs in visible locations at access points to video-surveillance areas. The sign must also indicate the purpose, for example with an image, must contain information regarding the data processor and the manner in which data subjects may exercise their rights.

In any case, the provisions of Article 22 of Organic Law 3/2018, of 5 December, on Personal Data Protection and the guarantee of digital rights must be considered.

For more information on the requirements and limitations for the capture of images for surveillance and security purposes, you may consult the Guide to the Use of Video Cameras for Security and Other Purposes prepared by the Spanish Data Protection Agency.

Question 4: I use a drone to capture footage that I view personally and I don't carry out any processing of images on the internet or with third parties. I only capture images of my family and me, even though on occasion I may capture images of spaces in which people live or persons passing through the spaces where I am recording. I understand that my activity is for family or domestic use and data protection regulations do not apply. Is that correct?

Answer: The activity described is exclusively for personal or domestic use insofar as it is carried out by a natural person and has no connection with any professional or commercial activity, in which case data protection regulations or the provisions of this guide do not apply.

In any case, one must take into account the obligation to respect private property (such as gardens, patios, terraces, interiors of residences, etc.) and all those areas in which there exists a reasonable expectation of privacy, including public areas.

There is a duty to make reasonable use of drones, ensuring the right to data protraction and people's right to honour and privacy, without prejudice to the provisions of any other applicable regulation based on the context of the activity that may be performed with a drone.

Question 5: I'm a model aircraft enthusiast and I use a drone for sporting or aeromodelling purposes. Sometimes I connect the camera and record the flight. I understand that this is private use and data protection regulation does not apply. My doubt is that sometimes I share images of my flights with other enthusiasts. If an identifiable person appears in these images, do I have to ask for consent?

Answer: This question is related to the previous one, as, in principle, this is a case of personal or domestic use, even where it is planned to operate the drone in public places.

The obligation to respect private property and the reasonable expectation of privacy must be stressed.

On the other hand, the domestic exception applies where images are captured without associating the images of subjects with any additional identification or indexation of contents of the recording, without carrying out any systematic monitoring of areas or persons (for example, using zoom or the creation of libraries of footage) and if the distribution is really of a nature limited to a domestic circle that does not affect people's rights and liberties.

Finally, as a responsible and respectful practice, it is recommended that, once the sporting or ludic purpose is complete, the footage containing identifiable persons is removed or those persons are blurred. The collection of data must be minimised when it does not affect the purpose of the activity, for example, by not adding audio or excessive resolution which allows post-processing.

REFERENCES

- http://ec.europa.eu/growth/sectors/aeronautics/rpas/
- https://www.seguridadaerea.gob.es/lang_castellano/cias_empresas/trabajos/rpas/default.aspx
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - RGPD)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen
- Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto

- Dictamen 01/2015 sobre la privacidad y la protección de datos en relación con la utilización de aviones no tripulados
- Informe jurídico de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales mediante la utilización de drones
- Study on Privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations
- https://www.aepd.es/media/guias/guia-videovigilancia.pdf
- https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf
- https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

www.aepd.es

@aepd_es