



aepd agencia
española
protección
datos



Drones y Protección de Datos

ÍNDICE

DRONES Y PROTECCIÓN DE DATOS	4
TIPOS DE OPERACIONES SEGÚN EL TRATAMIENTO DE DATOS	5
1. OPERACIONES QUE NO INCLUYEN UN TRATAMIENTO DE DATOS PERSONALES	6
2. OPERACIONES CON RIESGO DE TRATAMIENTO DE DATOS PERSONALES DE FORMA COLATERAL O INADVERTIDA	6
3. OPERACIONES QUE TIENEN POR FINALIDAD UN TRATAMIENTO DE DATOS PERSONALES	7
4. PASOS QUE DEBEN DARSE ANTES DE MANEJAR UN DRON	8
5. PREGUNTAS FRECUENTES	10
REFERENCIAS	12

DRONES Y PROTECCIÓN DE DATOS

La generalización del uso de drones en el ámbito civil y su crecimiento exponencial es un hecho indiscutible.

La configuración por defecto de cualquier dron incluye al menos un GPS y una cámara de video, y a partir de ahí se pueden añadir todo tipo de dispositivos de adquisición y procesamiento de datos como cámaras termográficas, cámaras de visión nocturna, escáner 3D, dispositivos WIFI y/o Bluetooth, sistemas de detección de dispositivos móviles, etc...

El derecho a la protección de datos es un derecho fundamental que garantiza la capacidad de cualquier persona a decidir sobre su propia información personal. El uso de drones con dispositivos como los que se mencionan en el párrafo anterior puede suponer o supone un impacto en el derecho a la protección de datos de las personas y, por lo tanto, puede implicar una lesión de sus derechos y libertades.

Teniendo en cuenta la definición de dato personal como “toda información sobre una persona física identificada o identificable”, los operadores de drones que registren y/o procesen imágenes, videos, sonido, datos biométricos, datos de geolocalización, datos de telecomunicaciones relacionados con una persona identificada o identificable están sujetos a la aplicación del [Reglamento General de Protección de Datos \(RGPD\)](#) y la [Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales \(LOPDGDD\)](#).

Hay que tener en cuenta que en ocasiones un dato puede identificar directamente a una persona como, por ejemplo, su fotografía, pero en otras ocasiones la identificación no es directa y requiere de un tratamiento adicional, como puede ser información de geolocalización, o

mediante el enriquecimiento con información adicional de otras fuentes como, por ejemplo, internet, y aunque a priori la persona no fuera identificable el resultado final sería que la identificación es posible gracias al cruce de informaciones de distintas fuentes. Tanto si el dato recogido mediante drones identifica inequívocamente a una persona como si su identificación se pueda realizar a posteriori, la normativa de protección de datos es aplicable.

La [normativa específica para la utilización del espacio aéreo](#) trabaja en paralelo con la normativa que defiende el derecho a la protección de datos personales de acuerdo con las obligaciones generales que señala el artículo 26 del [Real Decreto 1036/2017](#), de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, donde se establece la obligación de adoptar las medidas necesarias para garantizar el cumplimiento de lo dispuesto en materia de protección de datos personales y protección de la intimidad. Por tanto, además de las previsiones que establece la normativa aeronáutica mencionada, deberá tenerse en cuenta que el RGPD y la LOPDGDD son de plena aplicación a cualquier tratamiento de datos personales que tenga lugar con el uso de un dron con independencia del ámbito profesional o aficionado al que esté asociada la operación del dron.



TIPOS DE OPERACIONES SEGÚN EL TRATAMIENTO DE DATOS

Las principales aplicaciones con drones son la videovigilancia, la inspección de infraestructuras, levantamientos topográficos, inspecciones y/o tratamientos en agricultura de precisión, y otros servicios de fotografía y video (para cine y tv, servicios inmobiliarios, ...), servicios de acceso a internet, etc. Sin embargo, la disponibilidad de múltiples dispositivos de adquisición de datos y plataformas cada vez más avanzadas hacen previsible la aparición de numerosas aplicaciones.

Desde la perspectiva que atañe estrictamente a la protección de datos, las operaciones con drones se pueden clasificar en dos categorías principales según la finalidad de la operación.

De un lado están aquellas en las que la finalidad de la operación implica por sí misma un tratamiento de datos personales, como es el caso de la videovigilancia o la vigilancia de personas por cualquier otro tipo de sensor (por ejemplo, el seguimiento de dispositivos móviles) y, por otro lado, estarían aquellas operaciones en las que la finalidad de la operación a priori no incluiría el tratamiento de datos personales, como puede ser la inspección de infraestructuras, levantamientos topográficos, inspecciones del terreno y otros servicios de fotografía y vídeo pero que podrían, en un momento dado, tener impacto sobre el derecho a la protección de datos y la intimidad de las personas.

OPERACIÓN CON DRONES

A priori NO incluye el tratamiento de datos personales (inspección de infraestructuras, levantamientos topográficos, inspecciones y/o tratamientos del terreno, otros servicios de fotografía y vídeo)

3. Incluyen el tratamiento de datos personales de forma intrínseca (videovigilancia, grabación de eventos)

1. Sin riesgo de tratamiento de datos personales

2. Con riesgo de ocurrencia de tratamientos de datos personales de forma inintencionada y/o inadvertida

1. OPERACIONES QUE NO INCLUYEN UN TRATAMIENTO DE DATOS PERSONALES

Este tipo de operaciones son las menos frecuentes y en ellas se pueden incluir operaciones con drones con configuraciones muy básicas que pueden o no incluir sistemas de posicionamiento GPS para asistencia al vuelo, pero carecen o no hacen uso alguno de dispositivos de captación de imágenes, sonido o cualquier otro tipo de datos o información personal.

También pueden incluirse en esta categoría operaciones en el ámbito recreativo con drones provistos de GPS y cámaras, pero en las que el uso de las imágenes capturadas se restringe al uso doméstico o no permiten en ningún caso la identificación de una persona.

En estos casos:

- Antes de compartir en internet imágenes o videos capturados con un dron es necesario asegurarse de que no contienen imágenes o datos relativos a personas, vehículos, viviendas u otros objetos que puedan conducir a la identificación de sujetos, y en caso afirmativo anonimizarlas mediante técnicas de difuminado o similares.

Ejemplos:

- se utiliza una cámara de muy baja resolución que no capta una imagen definida del rostro de una persona de tal forma que permita su identificación, pero la imagen de esa persona aparece en su vivienda de manera que el lugar en el que aparece puede permitir su identificación.
- la imagen no permite identificar a la persona que conduce un vehículo, pero sí registrar su matrícula, lo que sí posibilitaría su identificación.

En ambos casos sería necesario llevar a cabo un postproceso o edición de las imágenes con el fin de impedir la identificación de las personas mediante técnicas de difuminado de las imágenes.

2. OPERACIONES CON RIESGO DE TRATAMIENTO DE DATOS PERSONALES DE FORMA COLATERAL O INADVERTIDA

En operaciones como la inspección de infraestructuras, levantamientos topográficos, inspecciones y/o tratamientos en agricultura u otros servicios de fotografía y vídeo (para cine, TV, publicidad, etc...); aunque no sea el objetivo de la operación, existe el riesgo de que se produzca la captura de datos personales forma inintencionada o inadvertida. Esto puede ocurrir bien porque sea inevitable capturar en segundo plano determinadas imágenes de personas, bien por la captura de otro tipo de información (viviendas próximas, zonas de recreo, vehículos, etc.) o bien por las características concretas de la operación, por ejemplo, la realización de operaciones fuera del alcance visual del piloto.

En estos casos es necesario observar las siguientes recomendaciones:

- Minimizar la presencia de personas y objetos que permitan su identificación (bañistas, matrículas de vehículos, transeúntes, etc.) en el lugar de la operación. Realizando los vuelos en horarios en los que no exista gran afluencia de público o controlando el acceso a la zona de vuelo si fuera posible.

- Minimizar la captura de imágenes a lo absolutamente necesario, reduciendo las posibilidades de que puedan aparecer personas inadvertidamente en las imágenes, y considerando la posibilidad de no capturar el vuelo completo, sino solo aquellos momentos que sean necesarios. Esta recomendación se puede extender a cualquier tipo de captura de datos.
- Promover y aplicar características de privacidad desde el diseño, como, por ejemplo, ajustar la resolución de la imagen al mínimo necesario para ejecutar el propósito del tratamiento, reducir la granularidad de la geolocalización con el mismo propósito; aplicar técnicas para anonimizar imágenes (automáticamente durante la captura o procedimientos para hacerlo inmediatamente después) o mecanismos para iniciar y detener la captura de datos en cualquier momento durante la operación; implantar protocolos de comunicaciones seguros que impidan a terceros el acceso a las transmisiones de los datos capturados o incluso al control del propio dispositivo, o incluir mecanismos que permitan el cifrado de los datos capturados y almacenados en el propio dron.
- Para lugares en los que inevitablemente habrá personas realizar la captura de imágenes de forma que las personas no puedan ser identificadas, por ejemplo, realizando capturas únicamente a distancia suficiente para que la identificación de estas no sea posible.
- Evitar el tratamiento de otro tipo de datos personales como, por ejemplo, la captura indiscriminada de identificadores de dispositivos móviles.
- Evitar el almacenamiento de información innecesaria relativa a personas. Por ejemplo, si las imágenes tienen por finalidad un levantamiento topográfico de una zona de costa, carecería de sentido almacenar imágenes que permitan la identificación de los bañistas que se encuentren en dicha zona.

3. OPERACIONES QUE TIENEN POR FINALIDAD UN TRATAMIENTO DE DATOS PERSONALES

Este es el caso de la videovigilancia, grabación de eventos o cualquier otra aplicación en la que la finalidad de la operación implica el tratamiento de datos personales de forma intrínseca.

En estas operaciones es de aplicación el RGPD y la LOPDGDD, así como lo establecido en la [guía sobre el uso de videocámaras para seguridad y otras finalidades](#) de la Agencia Española de Protección de Datos, donde se establecen las limitaciones a la videovigilancia a través de sistemas de cámaras o videocámaras o el seguimiento de identificadores de dispositivos móviles. En particular, se tendrá en cuenta, que la instalación de videocámaras en lugares públicos con fines de seguridad, tanto fijas como móviles, es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad.

Además, se hace necesario observar las siguientes recomendaciones adicionales:

- Sobre el rol del operador del dron:
 - Si el tratamiento se realiza por encargo de un tercero que decide acerca de la finalidad de las imágenes (por ejemplo, con propósito de videovigilancia), este tercero será el responsable del tratamiento, el operador del dron actuará como encargado de un tratamiento de datos personales y debe asegurarse de que su relación con el responsable esté regida por un contrato o un acto jurídico que lo vincule con el responsable y que actúe solo siguiendo órdenes de este. En materia de protección de datos el responsable es la persona que decide acerca de la finalidad del tratamiento mientras que el encargado es el que procesa los datos personales siguiendo las pautas e instrucciones marcadas en una relación contractual entre ambos.

Para más información sobre la elaboración de un contrato de encargo de tratamiento puede consultarse la guía sobre [Directrices para la elaboración de contratos entre responsables y encargados de tratamiento](#).

- Si el operador actúa como responsable: Deberá determinar la base jurídica más apropiada para llevar a cabo el tratamiento (consentimiento, contrato, obligación legal, interés legítimo, etc...). En general deberán cumplir las obligaciones a las que se refiere el RGPD.
- Elegir la tecnología a bordo más adecuada a la finalidad que se persigue con la operación y adoptar todas las medidas adecuadas de privacidad por defecto, evitando la recopilación y tratamiento posterior de datos innecesarios.
- Habilitar mecanismos para llevar a cabo el derecho de información con relación al tratamiento de datos personales que se realiza, teniendo en cuenta la peculiaridad de los drones pero sin olvidar que la información proporcionada deberá ser clara y transparente, y puede proporcionarse por medios electrónicos. Por lo tanto, se deberá de encontrar el modo más apropiado de informar a quienes van a verse afectados por el tratamiento de datos: informar mediante señalizaciones u hojas informativas, publicaciones en redes sociales, periódicos, folletos, pósteres, etc. en los que conste la identidad del responsable del tratamiento, su finalidad y se facilite a los afectados indicaciones claras y específicas para el [ejercicio de sus derechos](#).

Para más información, puede consultarse [la Guía para el cumplimiento del deber de informar](#).

- Tomar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos para los derechos y libertades de las personas, en particular para prevenir cualquier tratamiento no autorizado durante la fase de transmisión de los datos capturados.

- Eliminar o anonimizar cualquier dato personal innecesario lo antes posible tras la recopilación.
- Incorporar opciones de configuración respetuosas con la privacidad y funciones predeterminadas como parte de un enfoque de privacidad desde el diseño.
- Hacer que los drones sean lo más visibles e identificables posibles, con características asociadas al responsable, haciendo que el operador sea también visible e identificable como responsable del dron. En este sentido, cuando sean de aplicación, serán tenidos en cuenta los requisitos de identificación y matriculación a los que se refieren los artículos 8, 9 y 10 del Real Decreto 1036/2017.

4. PASOS QUE DEBEN DARSE ANTES DE MANEJAR UN DRON

Cuando sea de aplicación la normativa de protección de datos de carácter personal (ver preguntas al final de este texto sobre la excepción por tratamiento personal y doméstico) se debe:

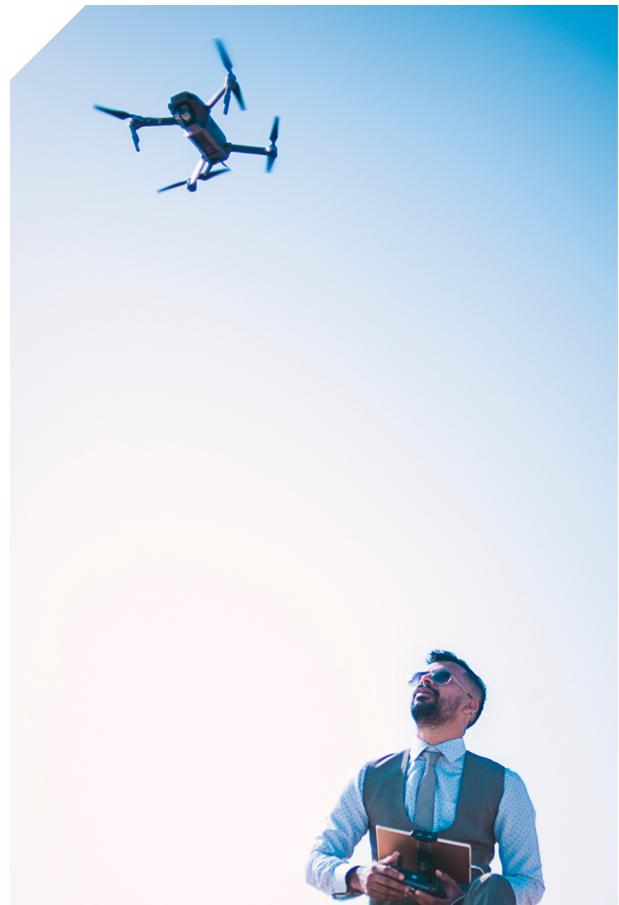
- 4.1** Comprobar si la legislación nacional permite manejar drones y si es necesario solicitar la autorización de las Autoridades Aeronáuticas. Cuando la operación de un dron viole la normativa nacional de aviación a la que está sujeta, o cualquier otra a la que deba atenderse, se considerará que la captación de datos y el tratamiento de los mismos realizado durante las operaciones aéreas no cumple con el principio de licitud recogido en el RGPD, y estará por tanto sujeto al régimen sancionador en materia de protección de datos (sin perjuicio además de que pueda estar sujeto al régimen sancionador en materia de navegación aérea u otros regímenes adicionalmente aplicables).

4.2 Al definir la campaña o servicio a ser ejecutado mediante drones, y con carácter previo al desarrollo de la operación en la que se pretende realizar un tratamiento de datos personales, se analizará la necesidad de llevar a cabo una evaluación de los riesgos que suponga el tratamiento para los derechos y libertades de las personas. En el caso de que el tratamiento esté dentro de los supuestos establecidos por el RGPD, o de la [lista de tratamientos](#) obligados establecida por la AEPD, será necesario [realizar una evaluación de impacto](#) sobre la protección de datos (EIPD) con la formalidad exigida en el RGPD. Si no existe obligación explícita de realizar una EIPD, llevarla a cabo siempre se considerará una buena práctica por parte del responsable del tratamiento. Ésta se realizará teniendo en cuenta el propósito de las operaciones, el tipo de drones y o las tecnologías de detección utilizadas. La evaluación de impacto se realizará para cada tipología de operación que se realice, aunque no es necesario llevar a cabo la evaluación tantas veces como se realice un determinado tipo de operación. Finalmente, si fuera necesario, se deberá realizar la consulta previa a la que refiere el artículo 36 del RGPD a la autoridad de control competente en materia de protección de datos.

4.3 Si del análisis de necesidad se llegara a la conclusión de que no fuera necesario realizar una evaluación de impacto, pero se pusiera de manifiesto la posibilidad de que la operación entrañe posibles riesgos para la protección de los datos personales de los afectados, se deberá llevar a cabo un análisis de riesgos con el fin de adoptar las garantías necesarias para paliar, en la medida posible, dichos riesgos y sus posibles consecuencias para los derechos y libertades de las personas. Para su realización se puede consultar la [Guía de análisis de riesgos de la Agencia Española de Protección de Datos](#).

4.4 Si se captaran imágenes para uso personal, es preciso tener en cuenta que no deben publicarse en internet de forma que puedan estar accesibles a un número indeterminado de personas cuando sea posible identificar a personas o cuando muestren espacios de uso privado como por ejemplo viviendas, jardines, terrazas, etc. Hay que tener en cuenta que incluso en aquellos casos en los que se trate de un tratamiento personal o doméstico al que no sea de aplicación la normativa de protección de datos, la información capturada por el dron, puede incidir en el derecho al honor, la intimidad personal y familiar, y a la propia imagen de las personas.

4.5 Evaluar previamente los objetivos de la operación garantizando la seguridad física del vuelo y cumplir con la normativa aeronáutica.



5. PREGUNTAS FRECUENTES

Pregunta 1: Mi cliente me ha encargado un trabajo para promocionar su hotel, he realizado un reportaje en el que aparecen huéspedes en las zonas del spa, piscina y en instalaciones deportivas ¿Puede mi cliente publicarlo en su página web? ¿Puedo publicarlo en YouTube para promocionar mis servicios de reportaje fotográfico?

Respuesta: En este caso tu cliente es el responsable del tratamiento de las imágenes que has capturado porque es quien decide sobre la finalidad de las mismas. Para publicar las imágenes de sus clientes en la web de su hotel necesitaría disponer del consentimiento expreso de dichos clientes, la ausencia del consentimiento podría significar una infracción del RGPD. Además, las imágenes de personas, por ejemplo, en zonas de spa o de piscina pueden afectar a su derecho al honor, a su intimidad y a su imagen, además de implicar un riesgo mayor con relación al derecho a la protección de datos.

Si se publican en YouTube, o en cualquier portal de acceso público, las imágenes de los clientes del hotel para promocionar tus servicios, estarás tomando una decisión sobre la finalidad de dichas imágenes y eso te convierte en responsable del tratamiento y, al igual que el propietario del hotel para el que trabajas, necesitarás el consentimiento expreso de todas y cada una de las personas cuyas imágenes vayas a publicar o añadir máscaras o pixelado para evitar que las personas sean identificables.

En este caso, lo recomendable es capturar las imágenes desde una distancia o con una resolución que impida identificar a las personas.

Pregunta 2: Soy un operador de drones contratado para la inspección de vías públicas. El dron utiliza una cámara y un dispositivo GPS para georreferenciar las fotografías que toma cuando detectamos un desperfecto en una calzada. En alguna ocasión captamos imágenes de las matrículas de los vehículos o incluso de sus ocupantes, entendemos que al no hacer un tratamiento de estas imágenes no es de aplicación la normativa de protección de datos.

Respuesta: La captación de imágenes de personas o de las matrículas de los vehículos y su grabación y almacenamiento implica un tratamiento de datos personales y, por tanto, se aplica la normativa de protección de datos.

Por ello, en primer lugar sería recomendable elegir una hora en la que exista menos tráfico con el fin de minimizar la grabación de imágenes de personas o de matrículas de vehículos. Si finalmente no fuera posible evitar la captación de imágenes de personas o de matrículas de vehículos, debería llevarse a cabo un post-proceso de imágenes destinado a eliminar cualquier dato que permita la identificación de las personas.

Pregunta 3: Utilizo un dron para videovigilar una propiedad ¿Dónde puedo ubicar el cartel de zona videovigilada?

Respuesta: Cuando un dron realice funciones de captación de imágenes con fines de videovigilancia de lugares privados, le será de aplicación el RGPD, y esto implica, entre otras cosas, la necesidad de cumplir con el deber de información del artículo 13, la realización de un registro de actividades de tratamiento, o la adopción de medidas de seguridad en función del análisis de riesgo realizado.

El deber de informar sobre el tratamiento de datos personales con fines de seguridad que incluyan captación de imágenes debe abordarse mediante carteles informativos en los accesos a las zonas videovigiladas y de forma visible. El cartel informativo, además de indicar la finalidad, por ejemplo, con una imagen, deberá contener información acerca del responsable del tratamiento y de la forma en la que los afectados pueden ejercer sus derechos.

En todo caso deberá de tener en cuenta lo previsto en el artículo 22 de la [Ley Orgánica 3/2018](#), de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Para más información sobre los requisitos y limitaciones para la captación de imágenes con fines de vigilancia y seguridad, puede consultar la [guía sobre el uso de videocámaras para seguridad y otras finalidades](#) de la Agencia Española de Protección de Datos.

Pregunta 4: Utilizo un dron para realizar grabaciones que visualizo personalmente y no llevo a cabo ninguna distribución de imágenes en internet o con terceros. Únicamente capto imágenes mías y de mi familia, aunque en ocasiones puedo capturar imágenes de espacios en los que viven personas o personas que transitan en los espacios en los que llevo a cabo las grabaciones. Entiendo que mi actividad se encuentra dentro de un uso familiar o doméstico y no le es de aplicación la normativa de protección de datos, ¿es correcto?

Respuesta: La actividad planteada es una actividad exclusivamente personal o doméstica en la medida en que se realiza por una persona física y no tiene conexión con alguna actividad profesional o mercantil, por lo que no le es de aplicación la normativa de protección de datos personales, o lo establecido en esta guía. En cualquier caso, hay que tener en cuenta la obligación a respetar las zonas privadas (tales

como jardines, patios, terrazas, interior de viviendas, etcétera) y de todas aquellas áreas en las que exista una expectativa razonable de privacidad, incluso en las zonas públicas.

Deberá de hacerse un uso responsable de los drones, garantizando el derecho a la protección de datos y el derecho al honor y la intimidad de las personas, sin perjuicio del cumplimiento de cualquier otra normativa que le fuera de aplicación en función del contexto de la actividad que pudiera llevarse a cabo con un dron.

Pregunta 5: Soy un aficionado y utilizo un dron con fines deportivos o de aeromodelismo. A veces le conecto una cámara y grabo el vuelo, entiendo que esto es un fin de uso privado y no es aplicable la normativa de protección de datos. A veces comparto con otros aficionados imágenes de los vuelos, por lo que si aparece alguna persona identificable en estas imágenes, me pregunto si tengo que pedir el consentimiento.

Respuesta: Esta pregunta está relacionada con la anterior, ya que en principio estamos en el caso de un uso personal o doméstico, incluso cuando se plantea operar el dron en zonas públicas.

Hay que insistir en la obligación de respetar las zonas privadas y en las que exista una expectativa razonable de privacidad.

Por otro lado, se estará acogido a la excepción doméstica siempre que la recogida de imágenes se realice sin asociar las imágenes de sujetos a una identificación adicional o indexación de los contenidos de la grabación, sin que se realice un seguimiento sistemático de áreas o personas (por ejemplo, mediante zoom o creación de bancos de grabaciones), y si la distribución tiene un carácter realmente limitado a un círculo doméstico que no afecte a los derechos y libertades de las personas.

Finalmente, como una práctica responsable y respetuosa, se recomienda que, una vez que el fin deportivo o lúdico se ha extinguido, se eliminen de las grabaciones aquellas partes que recojan a personas identificables, o que se difuminen. También que la recogida de datos se minimice cuando no afecte al propósito de la actividad, por ejemplo, no añadiendo audio o una resolución excesiva que permita un postproceso.

REFERENCIAS

- [Comisión Europea: industrias aeronáuticas](#)
- [Agencia Estatal de Seguridad Aérea](#)
- [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](#)
- [Guía sobre el uso de videocámaras](#)
- [Guía práctica para las Evaluaciones de Impacto en la Protección de Datos](#)
- [Guía práctica de análisis de riesgos para el tratamiento de datos personales](#)



 www.aepd.es

 [@aepd_es](https://twitter.com/aepd_es)