This Handbook is part of the project Dronerules.eu which has received funding from the European Union's COSME Programme (2014-2020)

DroneRules.eu
FOR PROFESSIONAL USERS

Privacy Handbook

1. What is this handbook?

This handbook is intended to be a useful guide to privacy and data protection risks that may arise when you operate drones for professional or commercial uses. Understanding and applying relevant laws will support you in responsible and sustainable drone use. This Handbook explains the concepts of privacy and data protection, as well as their requirements, specifically in the context of professional drone use. You will also find good practice ideas to assist with your responsible drone use, practical examples to aid you in better understanding the subject matter, together with some frequently asked questions.

2. Who is this handbook for?

This handbook is for individuals or companies who would like to utilise drones for commercial activities in their professional capacity. Groups of professional users that this handbook may assist include:

- If you are planning on using drones to provide a service or deliver goods, this Handbook will help you understand how to respect people's privacy and comply with the relevant privacy law in the EU.
- More specifically, if you are using drones in the context of precision agriculture, for surveying infrastructure, mapping an area, to record an event, capture cultural and historical sites, for rescue missions during emergencies or to use as wireless service providers, this Handbook, together with our case studies can help you grasp the privacy and data protection implications of your activities.
- If you want to use drones for environmental purposes or disaster or humanitarian relief, this Handbook will explain what you should be aware of in emergency situations.
- If you are a drone manufacturer, some privacy requirements during the manufacturing process will also be briefly explained.
- If you are offering flight training courses for drones, this Handbook can help you and your students understand some of the privacy and data protection principles of the EU.

If you plan on using drones, you should be aware of the privacy issues, including the data protection requirements, which may arise when you use drones. To save yourself time and potential legal troubles, consider consulting a legal professional and ensure that you take sufficient safeguards to protect the privacy of the people who happen to be around when you use drones. This handbook will help you better understand privacy and data protection, as well as how your activities could threaten them.

Please note, this Handbook is **not** aimed at the following groups of professional users:

- Law enforcement agencies – there are special rules in 2 European Directives on how law enforcement should handle personal data and privacy in the context of criminal offences and terrorism and serious crimes.
- Journalists – you should consult your national legislation, professional codes of conduct and guidelines, as well as your national professional association to understand how you should respect people's privacy.

To ensure that your commercial drone activities are in full compliance with the law, please consider the privacy implications of drones and take steps to minimise the risk presented by your use.

3. Why is this handbook important?

Due to the increasing ways in which drones can be used commercially and professionally, drones could impact the privacy of people around their area of operation. Drones can be equipped with a variety of payloads and have a lot of different uses, which means that they could, for example:

- Collect visual information through cameras, infrared sensors or thermal imaging equipment.
- Collect non-visual data, e.g. location data through the use of GPS or IP addresses if they serve as wireless connection platforms. Even this non-visual personal data can raise privacy issues.
- Can often remain unnoticed by people on the ground due to their varied size and mobility.

Because of the risks presented above (and others), you need to be aware of the different privacy concerns that varying drone usage raise and how to avoid them if you wish to use drones for commercial purposes in Europe.

4. What is Privacy?

In the EU, privacy is recognised as a fundamental human right. It is protected by national and European public bodies and individuals can protect themselves in court against privacy-invasive behaviour. The right to privacy is recognised as the fundamental right to respect for private and family life. More specifically, it is protected by the following Articles:

- Article 7 of the Charter of Fundamental Rights of the EU
- Article 8 of the European Convention of Human Rights

Everyone has the right to respect for his or her private and family life, home and communications. People have the right to act and speak without being observed in their homes or jobs, with their family and friends, and in their correspondence.

What do we mean by privacy?

People have privacy in their personal lives, homes, communications and opinions. Privacy is the freedom of people to choose what, how and with whom to share. The right to privacy empowers people to decide what is known about them. It allows people to act and think freely without fear of being observed, monitored or profiled.

People's location and personal context influence their reasonable expectations of how much privacy they have and they may change the way they act. However, no matter where people are – whether they are at home or in a public space, they have a right not to be targeted and followed.

DEFINITION

The right to private life means: the personal boundaries within which an individual operates freely and with a reasonable expectation of not being observed. These boundaries include home, personal relationships (family and friends) and selected fields of information (personal, sensitive or embarrassing information). Intrusions into this private life are illegal.

People have different reasonable expectations of their privacy in different contexts. Think about what is appropriate in every context and respect their privacy.

When do I have to comply with the right to privacy?

Since privacy is a fundamental right of all persons, you should always respect it. Whenever you use drones to carry out your professional/ commercial activity, you should take steps not to infringe the privacy of others.

5. Which of my activities could impact on privacy and how can I avoid infringing privacy?

Depending on your activities, location, drone payloads and the data you collect, your professional drone use can impact privacy rights in various ways.Your professional drone use can also trigger the application of data protection law.

The following will assist you in understanding how your use of drones could affect people's privacy.

COLLECTION OF IMAGES AND OTHER VISUAL DATA

Collection of images and other visual data - If people are captured in any images or footage you collect, this could harm aspects of their privacy. This is also true if you collect images through infrared or thermal technology! This could harm a person's:

- **Bodily privacy** - People have the right to keep aspects of their person and of their body private.
- **Privacy of data and image** - People have the right to control who has their data or their images and whether, how and why they can use them.

Do not take images of people when their bodies are exposed without their consent if they are in a private or a secluded location.

If you plan on taking images of a particular person, you should contact them, inform them and ask them for their agreement. Be mindful of the detailed rules of data protection law.

CAPTURING CONTINUOUS FOOTAGE

Targeting a person or capturing them for continuous periods of time – Capturing a single person/ specific group of persons for a prolonged period of time or if you target them specifically will raise privacy concerns.

Do not target, monitor and observe a person for prolonged periods of time without their knowledge and agreement, for example, by using a zoom lens or a directional microphone. This applies to both public and private spaces. Otherwise, you risk threatening a person's:

- **Privacy of location and space** - People have the right to move freely without being identified, tracked or monitored. This applies both to people's homes and some public spaces where they expect some privacy.
- **Privacy of behaviour and action** – People have the right to act freely both in public and in private without their actions being monitored or controlled by others.

As a rule, avoid collecting any kind of information about a person over prolonged periods of time without their knowledge and agreement!

CAPTURING INFORMATION THAT COULD REVEAL MORE ABOUT (AN) INDIVIDUAL(S)

Capturing information that could reveal more about (an) individual(s) – In particular circumstances, information which you happen to collect could make it possible to learn more about a person than simply their appearance or location. That could be, for example, if you capture images of religious buildings, political party establishments, or trade union offices. Assumptions can be made regarding a person captured walking in or out of such a building

Another issue could arise if your drone is used to transport communication between people in some way - via wireless networks or by delivering postal packages.

In these cases, you could threaten the following types of privacy:

- **Privacy of thoughts and feelings** - People have the right not to share their thoughts or feelings or to have them revealed. This includes their beliefs and opinions.
- **Privacy of association** - People have the right to associate with whomever they wish without being monitored. This includes meeting and interacting, as well as being part of a larger ethnic, religious or political group.
- **Privacy of personal communication** - People have the right to communicate in secret with whomever they wish. Accessing, recording or intercepting their communication without their consent or another legal requirement is not allowed.

Think about the areas where your drones will be operating and what information they may collect. Carefully consider if they may reveal personal and sensitive aspects of people's personalities and behaviours.

Information about individuals which relates to religious beliefs, political views ..... may be considered sensitive data and may require that you take additional safeguards if you collect it.

NOT BEING VISIBLE AND ACCOUNTABLE

Drones could remain undetected by individuals on the ground, especially if they are small, quiet and operated from a distance or fly autonomously. This means that individuals may not be aware if they are being observed and, even if they are being observed, they would not know who is operating the drone and why. This could raise issues with the transparency, visibility and the accountability of drone users.

How to avoid it? Make your drone more visible by painting it in a brighter colour. People must be able to see who is operating the drone so you could include your company's logo. Engage in a public information campaign through appropriate means, e.g. advertisements, signs, social media announcements, that inform people about your planned activities, including location and time. Inform people of what the drone will be doing, why, for whom and how people could contact you if they have any concerns or questions. If someone does not wish to be filmed, you should respect their wish.

What legal aspects should I be aware of? In the EU, data protection laws have laid down detailed rules on the accountability of people and companies if they collect and use data that may lead to the identification of (an) individual(s). This is data protection law.

Even if you inform people of what you will be using your drone for, you still have to comply with all other relevant principles of privacy and of data protection in all your activities.

Remember that you can be held accountable for any privacy infringements both by people and by public authorities in the EU!

BEING UNRECOGNISABLE

Using a drone without any identification and without engaging in an information campaign prior to your operation may leave people on the ground feeling insecure and observed, even if your drone does not carry any recording equipment. People would not know who is operating the drone and they may experience a **chilling effect**.

A chilling effect occurs when individuals perform a form of self-preservation / self-censorship by restricting their behaviour when they are, or believe that they are, being watched. Individuals may feel discouraged from participating in social movements, social gatherings, public dissent activities or any other related general exercise of their rights, such as freedom of assembly or freedom of expression. This can occur even in the mere presence of a drone, even if they are not actually being filmed by that drone.

How can it be avoided? – Be visible and contactable. By informing people of who you are and your activities, you give them more knowledge about the drone's use. People can then remain in control of what they are doing without experiencing any unnecessary fear.

Respect people and their dignity. Inform them of your activities and remain open to contactwith members of the public. This will relieve any fears people may have regarding your drone use.

CARELESSLY EXPANDING THE USES OF YOUR DRONE

If you start using your drone for additional reasons to what you first intended to do, you should be careful of the danger of performing function creep. **Function creep** refers to the possibility that a system which was originally intended for one purpose extends its operation to fulfil additional purposes at the discretion of the drone user. This could happen, for example, when a drone is originally used to map an area around a private residence but ends up capturing information that is later used for assessing the living standard of the people in the neighbourhood.

How can it be avoided? Keep a clear plan of what you will use the drone for and what you will do with any data you collect. Do not deviate from this plan.

What legal aspects should I be aware of? A function creep, when it involves people's personal data, could be contrary to the purpose limitation principle in data protection law and could make you legally accountable.

6. What is data protection law and why you need to know about it?

Like the right to a private life, the right to protection of personal data is also a protected fundamental right in the EU. It is protected by Article 8 of the Charter of Fundamental Rights of the EU. This means that dealing with any information about a person (personal data) that could allow his or her recognition or identification is subject to a number of legal principles that you must follow. The goal is to allow people control over who, how and why their personal data is collected and used by. They are given the right to ask you to delete personal data you have about them and limit how you can use it

If you are an **individual or a company** using drones for professional purposes/ commercial activities and you capture any personal data, you have to follow some detailed legal requirements. The EU has two legal acts which are important in this regard:

- The Data Protection Directive – this applies to your activities before May 2018
- General Data Protection Regulation – this applies to your activities after May 2018

For certain other bodies, there are specialised data protection laws. For example, if you are a law enforcement agency, make sure to be aware of the requirements of Directive 2016/680 and if you are a journalist, you should follow your national law. Consult your national professional association and national data protection authority if you would like further guidance.

Why is it important for you? Data protection law in the EU has strict requirements and principles that you need to follow. If you don't, you could be facing a fine up to 20 000 000 EUR or 4% of your worldwide company turnover.Individuals could also sue you and get compensation in court if you have harmed their data protection rights.

WHEN DO I HAVE TO COMPLY WITH DATA PROTECTION PRINCIPLES?

You must follow data protection laws if both of the following conditions apply to you and your drone commercial activities:

1. You are based in the EU or you operate your drones in the EU
2. You have collected in some way personal or sensitive data of a person (information that relates to an identified person or allows his or her identification).

Personal data could be a wide variety of information about people – their image, their location, their address, etc. If you captured people's faces or other information which allows the identification of a person, you will have to follow data protection principles.

Data protection law does not apply if the information you have captured is not personal. You could use anonymisation techniques to lessen the legal requirements on your commercial activities. But remember: this is not a full solution, sometimes people might still be identified from the context of the information you collected.

WHAT IS PERSONAL AND SENSITIVE DATA?

There are two kinds of data you should be aware of. If you collect either type of information, you will have to act in accordance with the data protection principles.

PERSONAL DATA - personal data means any information relating to an identified or identifiable person. Examples include an image, a name, a location, specific physical or physiological features.

A recording or other information you collect through a drone will contain personal data if **one of the following** is true:

- A person's face is clearly visible. However, if there are individuals in the distance and the faces are blurred, it is unlikely to be considered personal data.
- The person can be identified in another way – from the location, visible address numbers, car plate numbers, time of day, specific clothing, etc.
- It shows details about the person's bodily characteristics, behaviour, private life or his or her professional activities.
- It is used when making decisions on how to treat, act towards or evaluate that person.
- It focuses on or targets that particular person, especially if for a prolonged period of time.

SENSITIVE DATA - Sensitive data is personal data about people that reveals their race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, health condition, sex life or sexual orientation. This is also known as special categories of data. If you capture sensitive data, you must implement special safeguards.

It is always best not to capture sensitive data, but if that is unavoidable, you should only capture sensitive data when:

- The sensitive data is absolutely necessary for your activities
- You have informed people of your activities and what you will use the information for
- People have explicitly agreed to this
- OR, People are acting in a clearly visible way in public and you happen to capture it.

Even then, however, you should not willingly harm people by using this information and you should respect all data protection principles.

When operating a drone, consider the location and context of your activities. Some locations require you to be very careful due to the sensitivity of the information you could collect. This includes religious buildings, political establishments, specialised hospitals or clinics, or even sex worker streets such as "Red Light Districts" in countries where prostitution is legal.

7. What data protection principles and rights should I always respect?

BEFORE THE DRONE FLIES

Data protection by design and by default – As of January 2018, if you collect or use personal data, you are required to comply with the principle of data protection by design and by default. This means that you, as a drone manufacturer, designer, programmer or other, are required to consider all of the principles and rights in this section even before your drone activity. You should consider what technology to use and how to organise your activities in a way that would ensure you comply with data protection law. By default, you should keep to a minimum:

- the personal data you collect
- how much you process it
- how long you keep it for
- who can access it.

Even if you are not the one flying the drones in the end, when building and developing their technology, you should contribute to making them as little privacy intrusive as possible. Learn about privacy and data protection and consider it throughout your work.

BEFORE COLLECTING PERSONAL DATA

Inform people - Act with respect towards people and inform them of your activities through any channels you decide are appropriate. You should do so in an easy to understand, clear and plain language. In particular, inform them of:

- Who you are and how you can be contacted
- What you are doing and why, e.g. if you are carrying out infrastructure inspections, mapping or research exercises
- What purposes you will use the personal data for
- Who you may share the personal data with
- How long their data will be kept for or how that will be determined
- All the rights they have

Reason for data collection - To collect and use personal data legally, you should have a good reason for doing so. There are a two main ways you can ensure that:

- **Ask for consent or have an agreement:** Whenever possible, ask people for their permission (consent) if you plan on collecting information regarding them. You can also do that as part of a larger agreement or contract you have with them, for example if they hire you to film their wedding or deliver something to their doorstep via a drone.
  NB. Keep in mind that people have the right to change their mind at any time and you should respect that.

- **Legitimate or vital interest:** If your actions aim to protect a legitimate or vital interest, you could also collect personal data. If you accidentally capture images or other data relating to people in the area of your activities, your actions could still be lawful.

A legitimate interest means an activity that is important for the public, for example, you are conducting research or safety inspections of important electricity or water infrastructure.

A vital interest means that you are trying to protect a person's life or wellbeing, for example if you are using your drone to find hikers lost in the woods.

Data minimization: Limit the personal data that you collect by altering the way you use drones, for example by flying at lower or higher altitudes depending on the context. Any information you collect (and retain) should be adequate, relevant and necessary for whatever you are doing.

Here is an easy guide to the main things you should consider and three keywords remember:
INFORM, LISTEN, MINIMISE

INFORM

Whenever you capture or record any information about a person, especially clear images of their face, inform them about it.

LISTEN

Ask people what you can and cannot do with their information and comply with their wishes at any point in time. Get acquainted with the data protection rights people have.

MINIMIZE

Always think about how to use drones in a way that captures the least amount of data about people in the area of your operation. Use and share that data as little as possible and always with the permission of people captured in it.

AFTER COLLECTING PERSONAL DATA

Purpose limitation: After you have informed people and they have agreed, only collect and use personal data for the purposes that you planned to. If you want to do something new and different with the data you have, you generally have to inform people of that and get their agreement again.

Integrity and confidentiality: Keep personal data as securely as possible. Protect it against unauthorised or unlawful access or damage, using appropriate technology for your activities.

Storage limitation: Keep personal data only for as long as necessary. If you have captured personal data that you do not need, apply anonymisation techniques, such as blurring, to images or videos recorded as soon as possible. Delete any personal data which you no longer need.

Sharing data: Do not share the personal data you have collected with third parties without the consent of the individual concerned or a legal requirement mandating you to do so. This is also true if you plan on sharing the personal data with a person or a company that is based outside of the European Union. If you do share your data with other companies, make sure that they will also follow all relevant data protection principles.

A NOTE ON ACCIDENTAL PERSONAL DATA COLLECTION

If you have collected personal data accidentally, but still need to retain the footage for some of your other activities, you will have to treat the information very carefully and in accordance with all data protection principles.

Remember, when in doubt about what to do, always consult your national data protection authority.

RIGHTS OF PEOPLE

Right to object: When you are collecting data without the consent or the agreement of a person, they have the right to object. You should generally respect that decision.

Right to change their mind: If people have agreed to you capturing their personal information with your drone, they also have the right to change their mind at any point in time and you should respect their decision. You are protected, though. This will not make your activities up to that point illegal.

Right to access: People have a right to know what information you have collected and stored about them, and they have the right to access such information.

Right to receive a copy: People have a right to receive or make a copy of their personal data that you have collected.

Right to erasure: People have the right to ask you to delete any information you have regarding them and you should generally do so.

PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment is a way to assist you with your data protection obligations and in respecting people's expectations of privacy. If the nature of your commercial activities with drones is likely to result in a high-risk to the rights of individuals, such the systematic monitoring of publicly accessible areas on a large scale, you are required to carry out a data protection impact assessment under the GDPR, which involves the data protection elements of the broader PIA. The assessment should include:

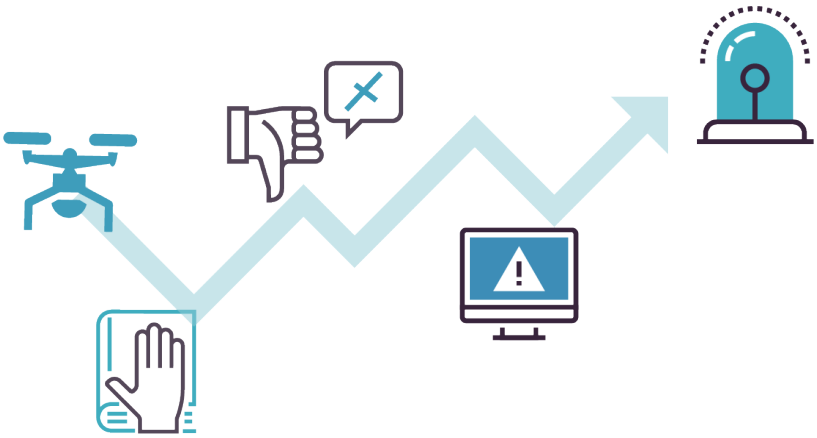
- A systematic description of how you plan to process personal data and for what purposes, including, if applicable, the legitimate interest you pursue
- An assessment of the balance between the purpose you pursue and the necessity and proportionality of the data processing
- An assessment of the risks that could arise to the rights and freedoms of people whose personal data you are processing
- Measures taken to address these risks (safeguards, security measures, etc.)

A data protection officer can aid you to prepare the impact assessment.

We have also prepared a Privacy Impact Assessment checklist, which is found here.

8. Understanding data protection risks – An introduction to relevant data protection law

Always remember:



- Professional drone use for commercial activity can threaten people's privacy and data protection, which are protected by law in the EU.

- The threat to privacy and data protection that a drone could pose would depend on its use, as well as what kind of equipment it has, e.g. microphones, cameras, GPS, etc.

- Privacy concerns can arise when using drones both in private, as well as public settings.Use your best judgment on whether or not people believe they are in a more private setting and respect their privacy accordingly.

- Activities that could especially threaten privacy include: the collection of images and other visual data; the capture of a particular person over a prolonged period of time; and/ or capturing information that could reveal very personal aspects about people, including their religious or political beliefs.

- Drones could cause people to be concerned about their privacy even if they are not equipped with a camera. Remember to be as transparent and visible as possible.

- Data protection concerns arise when you collect information that allows the identification of people. Remember that sometimes people could be identified from the context of the capture, even if their faces are not clearly visible.

- If you have captured a person's image with a clearly visible face, that is considered personal data. You will have to follow data protection principles to ensure you comply with the law.

- Think of the best way for you to use drones in your professional/ commercial activities without capturing private aspects of people's lives. In any event, always:
  - Inform people of your activities
  - Ask them for their consent, if you believe they will be captured
  - Treat the collected information securely
  - Comply with their wishes on what you can and cannot do with the information.

- Do not target and pursue a specific individual in your activities without their knowledge and consent.

- Do not share the information of anyone with third parties unless that person has consented to it.

- Before you use the personal data of anyone for any purpose, make sure they know what you want to use it for and that they agree to it. Do not use the data for anything else.

This Handbook is part of the project Dronerules.eu which has received funding from the European Union's COSME Programme (2014-2020)