DroneRules.eu PRO

Privacy Code of Conduct:

A practical guide to privacy and data protection requirements for drone operators and pilots

This work
is funded by the
European Union's
COSME Programme
(2014-2020).

TABLE OF CONTENTS

1 PURPOSE OF THE CODE

This Code of Conduct is intended to help guide the activities of drone operators and drone pilots as they carry out professional commercial activities using drones. The Code can help companies plan their activities and establish a formalised set of rules for the conduct of their employees so as to minimise their impact on the privacy of individuals and to facilitate compliance with the requirements set out by the General Data Protection Regulation (GDPR).

This Code constitutes a set of standards for drone professionals across Europe, intended to help guide them in carrying out their everyday activities. This Code is intended to form a basis on which the drone industry can collaborate and build a GDPR-recognised Code of Conduct for the drone sector pursuant to Article 40 GDPR, which could help drone pilots and operators comply with the GDPR through guidance and serving as proof of compliance. For further information as to how to receive approval for a Code of Conduct pursuant to Article 40 of the GDPR, please see the Section "This Code as an Article 40 GDPR Code of Conduct" below.

This present Code is not a legally binding document and should be used as a source of guidance and knowledge together with the other resources available on the DroneRules.eu website. This Code can be an instrument of voluntary compliance. Drone pilots and operators, wishing to subscribe to the Code, can do so voluntarily through

(1) Self-assessment of compliance with the Code and self-declaration of compliance

or

(2) Certification by independent third-party auditors.

2 THIS CODE AS AN ARTICLE 40 GDPR CODE OF CONDUCT

This Code of Conduct can serve as general guidance of good practice and practical tips, do's and don't's for drone pilots and drone operators in Europe. This Code is built on extensive research of both GDPR requirements, as well as requirements of the right to privacy. You can, therefore, rely on this Code in its present form as a guidance document

of all principles, obligations and individual rights which you, as a drone pilot or operator, should consider and ensure during your flight planning, flying and subsequent handling of data collected up until the moment of the data's complete anonymisation or erasure.

This Code can also form the basis of a legally recognised Code of Conduct pursuant to Article 40 GDPR, which could then serve to alleviate the compliance burden of drone professionals adhering to it by offering tailored and practical guidance and clarification as to their obligations under the GDPR. To achieve the status of a Code of Conduct pursuant to Article 40 GDPR, drone industry associations and representative organisations (or a working group of representatives of such bodies) are encouraged to take up this Code of Conduct and further develop the following aspects of it:

- Include procedures for making the Code of Conduct legally binding and enforceable on parties that want to adhere to and benefit from it, for example by incorporating it into a legal agreement to be signed among participants in the Code of Conduct.
- Create procedures and structures to ensure that data controllers and processors wishing to adhere to and benefit from the Code actually comply with the Code. The Code should have clear guidelines on the procedures and requirements for joining the Code of Conduct and for withdrawing from it.
- If deemed appropriate, the application of the GDPR can be clarified with regard to out of court dispute resolution procedures[1] that the drone sector has committed to.
- Designate an independent body with expertise in the sector and in the Code of Conduct, accredited by the competent supervisory authority, to monitor compliance with the Code.[2] Among other qualities, such a body should have:
    - Procedures to assess the eligibility of controllers and processors wishing to apply the Code,
    - Procedures to carry mandatory monitoring of their compliance with the Code,[3]

[1] Article 40(2)(k) GDPR.
[2] Article 41 GDPR.
[3] Article 40(4) GDPR.

- Procedures to periodically review the operation of the Code,
- Procedures and structures to handle complaints about infringements of the code or the manner of implementation of the Code and to make these procedures transparent to the public and data subjects.

In further developing these aspects, industry representatives should take account of the particular needs and practices of their members and constituents, (micro and) SMEs and industries likely to be users of drone services and all other stakeholders that may be relevant.[4]

In addition to creating procedural and governance structures of the Code of Conduct and further developing and amending any principles and requirements they deem necessary, representative organisations from the drone sector should seek the approval of the code by their competent supervisory authority.[5] To have the Code recognised as a means of compliance for personal data processing carried out all over the European Union or across a number of Member States, the competent supervisory authority will refer the Code to the European Data Protection Board[6] (EDPB) for its opinion and approval. If the opinion of the EDPB is positive, the European Commission may then recognise and give legal status to the Code of Conduct by adopting it as an implementing act.

3 GLOSSARY

The terminology used in this Code of Conduct is intended to have the same meaning as ascribed to it in the GDPR or in the EASA Draft Commission laying down rules and procedures for the operation of unmanned aircraft.[7] In case of conflict between the

[4] Article 40(1) GDPR.
[5] Article 40(5) GDPR.
[6] Article 40(7) GDPR.
[7] Draft Commission Regulation (EU) laying down rules and procedures for the operation of unmanned aircraft, available at: https://www.easa.europa.eu/sites/default/files/dfu/DRAFT%20COMMISSION%20REGULATION%20%28EU%29%20...-...%20laying%20down%20rules%20and%20procedures%20for%20the%20operation%20of%20unmanned%20aircraft.pdf.

definitions of these legal documents, precedence should be given to the meaning allocated within the GDPR. The following terms are used in the Code of Conduct:

- 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[8]

- 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;[9]

- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others (called joint controllers), determines the purposes and means of the processing of personal data;[10]

- 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[11]

- 'involved person' means someone who can reasonably be expected to follow directions and safety precautions given by the person controlling the operation, in order to avoid unplanned interactions with the UA.[12]

[8] Article 4(1) GDPR.
[9] Article 4(2) GDPR.
[10] Article 4(7) GDPR.
[11] Article 4(8) GDPR.
[12] GM1 UAS.OPEN.030(1) and UAS.OPEN.040(1) Definition of 'uninvolved person', EASA Draft Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Regulation laying down rules and procedures for the operation of unmanned aircraft and to Annex (Part-UAS – UAS operations in the 'open' and 'specific' categories), available at:

4 GUIDELINES

The following set of guidelines will help drone pilots and drone operators respect privacy and consider data protection while planning and carrying out drone operations, as well as when managing any personal data collected. It is important to incorporate these guiding principles in internal company documents (e.g. the Operations Manual), procedures and policies, as well as to dedicate sufficient resources and encourage compliance by personnel with procedures. The support and commitment of management to achieve the effective implementation of these guidelines is paramount to ensure respect for these principles in practice. The practical implementation of these guidelines in regular business practices and the undertaking of legal commitments to comply with them is encouraged.

4.1 Establishing a legal framework for drone activities

4.1.1 Clear frameworks for legal responsibilities

Responsibilities of the drone operator as a data controller

DO Where the drone operator is a data controller of personal data, they will carry full responsibility for complying with the principles and requirements of the GDPR.

Data controllers should implement all necessary steps to ensure that:

- drone operations are carried out with the least interference with the privacy and personal data of individuals on the ground possible;
- personal data collected is handled in compliance with the principles, requirements and individual rights laid down in the GDPR;
- data processing activities are duly documented, ensuring accountability and transparency for the data controller and their compliance with the GDPR;
- where legally required, a Data Protection Impact Assessment (DPIA) is carried out and a Data Protection Officer (DPO) is appointed, in accordance with Articles 35 and 37 GDPR (national laws stipulate additional scenarios where a DPO has to be appointed);
- any data processors engaged are clearly instructed how to process personal data and capable of ensuring that personal data is handled securely and in accordance with the GDPR.

https://www.easa.europa.eu/sites/default/files/dfu/Draft%20AMC%20%20GM%20to%20draft%20Regulation%20...-...%20and%20to%20the%20draft%20Annex%20%28Part-U....pdf.

DO A data controller should ensure that personal data is handled with due care in the hands of third parties. Where data is shared with external parties, including data processors, an agreement setting out the rights and obligations with regard to the sharing of personal data (e.g. Data Processing Agreement) should formalise the data processing.

Responsibilities of the drone operator as a joint controller

Where a drone operator is a joint controller of personal data, e.g. with a client who has enlisted their services, all joint controllers will be jointly and severally liable to ensure that the personal data processing carried out is in full compliance with the requirements of the GDPR. Each of the joint controllers carries the same responsibilities as a sole data controller.

DO Joint controllers should clearly allocate the responsibility regarding ensuring compliance with the GDPR in a Joint Controller Agreement[13], whereby each data controller should carry full responsibility for ensuring personal data within their possession is handled in a manner, compliant with the GDPR and, when personal data is held by a drone operator, in compliance with this Code of Conduct.

Responsibilities of the drone operator as a data processor

Where a drone operator acts as a data processor on the detailed instructions of a data controller of personal data, e.g. with a client who has provided strict specifications about the flight path and/or the way data is to be collected during a drone operation and the client exercises ultimate approval and decision-making power, the drone operator carries legal responsibility to ensure that:

- the instructions of the data controller are complied with;
- the security of the personal data processed is guaranteed and where data breaches take place, the data controller is immediately informed;
- all necessary information and support are provided to the data controller when requested, including for the purpose of carrying out a Data Protection Impact Assessment pursuant Article 35 GDPR;
- a DPO is appointed where legally required pursuant to Article 37 GDPR.

DO Where the drone operator / pilot is a data processor, they should receive clear instructions for the processing of personal data from a data controller through a type of Data Processing Agreement pursuant to Article 28 GDPR – also called Controller-Processor-Agreement.

TIP Where the drone operator / pilot act beyond the instructions of the data controller, they will be considered a data controller for that processing and they will carry full responsibility to ensure personal data is handled in compliance with the GDPR. Where a data processor does not enter into a Data Processing Agreement with the data controller, it cannot rely on being a data processor but will be deemed as data controller, too.

[13] Article 26 GDPR.

4.1.2 Legal framework for personal data processing

Processing personal data lawfully

A legal basis is necessary whenever personal data is processed during a drone operation.

DO Where a drone operator acts as a data controller, they are responsible for basing their personal data processing activities on a legitimate legal basis pursuant to Article 6 GDPR. A legal basis shall be determined for each group of compatible (related) purposes of data processing. Personal data should be processed only as far as necessary for the fulfillment of the legal basis.

When determining the appropriate legal basis for personal data processing account should be taken of the nature and context of a drone operation, its purpose and the relationship between the drone operator or pilot and individuals. The choice of a legal basis should be carefully considered, as it cannot be easily changed once data processing begins.[14]

TIP Where a drone operator or pilot acts as a data processor, they should ensure that the data controller has considered and established a legal basis for the processing of personal data. While this may not be a requirement of the law, it will shield operators and pilots from potential joint liability under Article 82 GDPR for any unlawful personal data processing.

TIP As per Article 6 GDPR, personal data may be processed where this is:

- based on an informed and explicit consent by individuals being captured;
- necessary for the fulfilment of a contract with the individual being captured or in order to take steps at the request of the individual being captured prior to entering into a contract (e.g. demo recording to demonstrate capabilities);
- necessary for compliance with a legal obligation to which the controller is subject;
- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- necessary to protect the vital interest of an individual;
- necessary for the legitimate interests of the data controller (whether this is the drone operator or a client of drone services) and proportionately safeguarding the rights and freedoms of individuals.

Processing special categories of personal data lawfully

Drone operators may also collect and process special categories of personal data, such as data related to individual's health, political or religious beliefs, sexual orientation or

[14] Information Commissioner's Office, "Guide to the General Data Protection Regulation GDPR: Lawful basis for processing". https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.

criminal convictions. Where this is the case, data controllers are responsible to ensure there is a legal basis for such processing pursuant to Articles 9 or 10 GDPR.

TIP Consider the location and context when operating a drone. Special categories of personal data are more likely to be captured in certain locations, e.g. near a hospital, political establishments, religious buildings, sex health centres, prisons or police stations. You may have to take special precautions if you operate near such locations.

TIP Special categories of personal data may be processed under a set of circumstances, including where:[15]

- this is based on an informed and explicit consent by individuals being captured;
- the personal data in question is manifestly made public by the individual concerned;
- the personal data is processed to protect the vital interest of an individual and acquiring consent by data subjects is not possible.

DO Where special categories of personal data are captured by drones operating over public areas, such data should not be shared further without due consideration of the potential impact of such sharing on individuals concerned and without a legitimate reason. Any personal data captured should be anonymised as soon as it is no longer necessary for the purpose of the drone operation.

Clear and specific purpose for personal data processing

DO A clear, specific, explicit and legitimate purpose for drone operation(s) and for capturing and processing personal data during the operation(s) should be determined. Personal data should be processed only where this is necessary for achieving the stated purpose(s).

DO Where drone services have been hired by a client, the clear and specific purpose of the drone operation should be discussed and determined together with the client.

Drone operators and drone pilots should be aware of the purpose of the drone flight and of collecting personal data, regardless of their roles as either data controllers or data processors.

Having a clear and specific purpose:

- is a legal requirement;[16]
- can serve as a guide to fulfil the requirements of data minimisation, purpose limitation and transparency, discussed later;
- can prevent drone operations from expanding unlawfully beyond their original plans.

[15] Articles 9(2)(a), (e), (c) GDPR.
[16] Article 5(1)(b) GDPR.

DON'T The collection of personal data without a specific (legitimate) purpose (e.g. to have "data in stock" for the future) is forbidden under the GDPR.

Documenting the legal basis and purpose of personal data processing

DO It is the responsibility of a data controller to prove that they act lawfully and document the legal basis of the personal data processing. [17] A data controller should:

- record the legal basis for each processing purpose and the reasoning behind choosing that legal basis;
- include the legal basis for personal data collection in the drone operation's Privacy Notice. Where personal data is processed on the basis of the data controller's legitimate interests, these interests should be clearly stated.

4.2 Be informed and plan with privacy in mind

4.2.1 Privacy by default and by design in drone operations

Incorporate privacy and data protection into drone operations and data handling practices

DO When planning a drone flight, drone operators and pilots should consider and aim to minimise their impact on the privacy and personal data of people on the ground within the design and default settings of their operation.

Interference with privacy and data protection rights should be minimised when planning (1) the flight path intended, (2) the drone and equipment used, and (3) the management of collected data.

Flight	Drone equipment	Data management
•Where and when should the flight be? •What is the surrounding area of the flight like? •What information should you disseminate, to whom and how before, during and after your flight? •When should data sensors be engaged and when should data be recorded?	•What equipment / functionalities should the drone have? What equipment is not necessary but excessive? •How will the security of data and drone be guaranteed? •How will the data collected be minimised? •Do pilots understand the equipment and how to best operate it?	•How will collected data be handled safely and securely? How will data be stored and transmitted? •How will personal data collected be minimised? How and when will personal data be anonymised or erased? •Who will personal data be shared with? Under what conditions?

[17] Article 5(2) GDPR.

TIP The *DroneRules PRO Privacy Impact Assessment (PIA) template* can serve as a guide through a step-by-step consideration of the risks of your operation how to mitigate them.

TIP The *DroneRules PRO Data Protection Impact Assessment (DPIA) template* can, furthermore, support drone operators and pilots through the process of a DPIA, required by Article 35 GDPR. The template can help operators and pilots determine whether they need to carry out a DPIA, after which it can guide them through a series of strategic and tailored questions to complete the process.

4.2.2 Tailoring drone operations to location and context

Identification of location and context of drone flight

DO Drone operators and pilots should inform themselves of the area in which the drone flight will take place. They should recognise the different types of locations and plan how to fly over or near them, as well as how to inform people of their activities appropriately and effectively.

Special steps and limitations should be considered to minimise privacy and personal data interference when flying over or near private and sensitive spaces.

Operating over public spaces

When operating in public spaces (e.g. streets, parks), drone operators and pilots should not target, follow and/or systematically capture people without their knowledge and consent.

Drone operators and pilots should avoid operating in the same location for a prolonged period of time unless this is necessary for the purpose of the drone operation and based on a legal basis.

When flying in the same location for a prolonged period of time, drone operators and pilots should take steps to minimise people captured and clearly inform persons living, working and passing in the area of the details of their drone operation and remain visible at all times.

Operating over private spaces

When flying near private spaces, such as homes, terraces, gardens, and private vehicles, drone operators and pilots should minimise their flight path over and near such locations.

Drone operators and pilots should plan flight paths and angles at which data is captured by drone sensors in a way to minimise the risk of capturing people within their private homes, business premises or inside their vehicle, unless this is necessary for the purpose of the drone operation and based on a legal basis.

Drone operators and pilots should also ensure they do not disturb persons in their private property and do not breach any relevant nuisance laws in the country of the drone operation. In any event, drone operators and pilots should not fly over private properties at altitudes lower than 20 m without the consent of the owners or tenants of the property.[18]

Operating over sensitive spaces

When flying over or near sensitive buildings, drone operators and pilots should seek to minimise their impact on individuals in the area. Sensitive spaces can be:

- spaces where vulnerable persons can be found, such as children, elderly, mentally ill people, refugees or prisoners, e.g. schools, kindergartens or playgrounds, elderly homes, refugee centres, prisons;
- places where sensitive or potentially embarrassing information about the people entering or exiting could be revealed, such as religious buildings, political party headquarters, hospitals or clinics.

Drone operators and pilots should plan flight paths and angles at which data is captured by drone sensors in a way to minimise the risk of capturing people inside or entering/exiting such buildings or locations, unless this is necessary for the purpose of the drone operation.

Drone operators and pilots should plan the time of their flight, e.g. time of day and day of the week, in a way to minimise the risk of capturing individuals in these locations. For example, operating near religious buildings at times of prayer should be avoided, unless necessary for the purpose of the drone operation.

Where possible, drone operators and pilots, wishing to fly in the vicinity of sensitive spaces, should inform responsible representatives of such locations the details of their drone operation and remain clearly visible at all times.

Where it is likely that special categories of personal data will be captured during a drone flight over or near sensitive spaces, drone operators and pilots, when acting as data controllers, should ensure that they act with a suitable legal basis pursuant to Articles 9 and 10 GDPR.

[18] GM1 UAS.OPEN.070(3)(h) and UAS.SPEC.070(3)(f) Respect for other people's privacy rights minimises any nuisance caused to other persons or animals, https://www.easa.europa.eu/sites/default/files/dfu/Draft%20AMC%20%20GM%20to%20draft%20Regulation%20...-...%20and%20to%20the%20draft%20Annex%20%28Part-U....pdf.

Areas restricted for drones

Drone flight over certain areas may be restricted by national airspace regulations for safety or security reasons[19] and, in some cases implemented through the use of geo-fencing. Such locations could include airports, critical infrastructure sights, gatherings of people, areas where an emergency response is in progress and dangerous areas.

Drone operators and pilots should seek information about such restrictions before flight and comply with them when planning and carrying out drone flights.

Where areas restricted for drones are designated through geo-fencing, drone equipment with geo-awareness capabilities and up-to-date databases of geo-fenced locations should be used to help comply with the restrictions while planning flights.

4.3 Act fairly, transparently and proportionately

4.3.1 Minimise the impact on people's privacy and personal data

Collect only the data necessary

Drone operators and pilots should plan and execute drone flights in a manner which minimises the collection of personal data to the personal data that is necessary for the purpose of the drone operations. Where data subjects have consented to being captured by a drone, drone pilots and operators should act within the limits of such consent and its conditions.

DO Drone operators and pilots should seek to capture the minimum amount of personal data and the minimum quality of personal data necessary for the purposes of the drone operation. This requirement extends to the type of sensors used, their power, the type of data collected, as well as the type of flight path chosen.

If it is possible to carry out a drone operation and achieve its purpose without collecting personal data, drone operators and pilots should do so.[20]

TIP To minimise personal data captured and the degree of interference with privacy, drone pilots and operators, where possible, should:[21]

- fly in a way to capture and/or record data about uninvolved persons on the ground as little as possible;
- use sensors of lower capabilities or tailor data quality through software controls;

[19] EASA EU Opinion No 01-2018, p.1.
[20] Information Commissioner's Office, "Guide to the General Data Protection Regulation GDPR: Lawful basis for processing". https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.
[21] Data Protection Commission, "Guidance on the use of Drones". https://www.dataprotection.ie/docs/Guidance-on-the-use-of-Drone-Aircraft/1510.htm

- control which drone sensors are engaged during flight and when;
- control when data is recorded and when it is streamed;
- capture images rather than video;
- use a secured livestream rather than recording data;
- use alternatives to photographic imaging, e.g. thermal imaging;
- fly at a higher or lower altitude, depending on the circumstances, to minimise the impact on people on the ground.

TIP Drone operators and pilots should remain up to date and informed about different technical solutions which could aid them in achieving data minimisation.[22]

Choose equipment to minimise personal data collected

When choosing drone equipment, drone operators and pilots should choose equipment which will allow them to minimise their impact on people's privacy and comply with data protection requirements.

In addition, where a drone flight takes place near uninvolved people and especially where it takes place over or near private or sensitive spaces, drone equipment should have software capabilities to control:

- which sensors are engaged, e.g. visual, thermal, audio, geo-location, and when sensors are engaged or inactive during flight;
- what direction drone sensors are pointed at or what angle they operate at;
- what quality of data (e.g. resolution, sensitivity of sensors) is captured; and/or
- when data captured is recorded and when not.

Drone pilots should be capable of operating the chosen drone equipment safely and effectively control it in a way to minimise the personal data recorded to what is necessary for the purpose of the drone operation.

4.3.2 Act visibly and transparently

Inform the people and the public

People should be aware if there is a drone operating around them. In fact, people have a right to be informed about the processing of their personal data and, out of respect for their privacy, people should be informed of any potential interference with their privacy by drone operations.

[22] For example, some platforms and technical solutions allow the automated blurring of faces of individuals, prevent the collection of data when a drone diverges from a predetermined path or prohibit a drone from entering spaces previously identified as private.

DO Drone operators and pilots should inform the public and especially the individuals in close proximity to drone operations of the nature of the drone operation, as well as relevant details surrounding the treatment of personal data captured. Attention should be paid to informing people of their rights and how they can exercise them and contact the relevant drone operator or pilot.

In particular, inform people of the following:

- the identity / company name of the drone operator and contact information of representatives;
- the nature, dates, times, duration and locations of drone operations;
- the purpose of the drone operation and the use of data collected;
- the legal basis (or bases) of personal data processing and/or the legitimate interests pursued;
- the categories and types of data to be collected (images, radio, location, etc.);
- subsequent processing of the data, retention period and erasure / anonymisation;
- the rights individuals have with regard to their own personal data, including their right to lodge a complaint with a relevant supervisory authority.

If you plan on sharing data with third parties, include information about:

- the potential data recipients and the purpose of sharing data with them;
- whether transfers to third countries or international organisations will take place and under what circumstances and safeguards.

DO All this information should be compiled in a single Privacy Notice document which is publicly available, clear and easy to understand, and reflects your treatment and use of personal data. A Privacy Notice should be prepared for every drone operation and individuals impacted by the drone operation should be referred to this document.

DO In all communications with the public, clear, concise and understandable language should be used.

Use a variety of channels to communicate with the public

Drone operators and pilots should use a variety of communication channels to inform people about upcoming and ongoing drone operations, as well as to refer them to relevant Privacy Notices, detailing the treatment of any personal data collected. A variety of communication channels should be chosen so as to be effective in informing relevant persons.

DO Whenever possible, drone operators and pilots should choose to use drone equipment with an electronic identification transmission, which is capable of enhancing the visibility and accountability of the drone operation by continuously transmitting the drone operator registration number, the unique serial number of the drone or the electronic identification add-on, the geographical location of the take-off

point of the drone, as well as the current location and altitude of the drone with an accurate time-stamp.

TIP Available communication channels include:

- posters or billboards close to the flight location;
- adverts in media, such as local newspapers or targeted online media campaigns;
- flyers and leaflets;
- up-to-date easily understandable information on the website of drone operators and their social media channels;
- orally provided information, during your operations.

TIP When seeking to communicate with people in the area of the drone activity, drone operators should consider appropriate partners to maximise the reach of their messages. Drone operators should seek to inform and cooperate with:

- local institutions or authorities in the area;
- local businesses or establishments;
- local associations, organisations, clubs;
- owners and proprietors of private property in the area;
- organisers of events in the area.

The effort and costs exerted to inform individuals of the drone operation should be proportionate to the risks to the personal data and privacy of individuals. In considering what is proportionate, drone operators should consider:

- the location and context of the drone operation;
- the likelihood that personal data and/or individuals will be captured;
- the amount and type of data related to individuals that is collected.

Be noticeable during flight

When flying, drone operators and pilots should do so in a visible manner that allows people to know that there is a drone operating, as well as who is operating it.

In particular, drone equipment should be visible, marked in a bright colour and/or with a logo of the drone operator.

Drone launch sites and the location of the piloting team should be clearly marked, visible and accessible. The piloting team at the location should be identified and available to answer any questions and concerns by people.

TIP To fly in a visible manner, drone operators and pilots should consider how to distinguish their drone equipment and launch location, including:[23]

- use lights to draw attention to the drone and indicate that it is recording;

[23] Privacy Comissioner for Personal Data, Hong Kong, Guidance on CCTV Surveillance and Use of Drones, March 2017. https://www.cityu.edu.hk/vpad/CCTVpractices_e.pdf.

- clearly mark a drone with the drone operator's corporate logo or painting it in its corporate colours;
- add contact details on the drone;
- have pilots / team members wear matching colour clothes or logos with names and identities;
- place pilots and crew members in a clearly located space outside and marking it as a launch sight, for example through banners.

DO In addition to taking the above steps, drone operators and pilots should ensure that, when required by aviation rules, a drone is registered with the appropriate authorities, as well as that it is equipped with electronic identification capabilities.

4.3.3 Respect the rights of individuals

Be informed about the rights of individuals and their extent

Individuals have the right to privacy. They have the right to be left alone, not to be observed, analysed or targeted, both in private and public spaces.

In addition, the GDPR lays down in law a set of rights which individuals have with regard to their personal data. These are:

- right of access
- right to rectify personal data
- right to erasure
- right to restrict processing
- right to data portability
- right to object
- rights in relation to automated decision-making and profiling.

DO As these rights are not absolute, drone operators and pilots should be informed about when these rights apply, the full extent of individual rights and how to respect them, including by establishing detailed procedures and guidelines.

This Code of Conduct will introduce the requirements of the rights most relevant to the drone industry – the right to access, right to data portability, right to object, right to erasure, and right to restrict processing.

Right to access

Individuals have the right to access their personal data.[24] Whenever individuals exercise their right of access to their personal data, drone pilots/operators should comply with such a request and provide them, in response, with information about:

[24] Article 15 GDPR; Article8(2) EU Charter of Fundamental Rights.

- whether their personal data is being processed,
- what kind of data is being processed and how it is being processed,
- for what purpose is data processed,
- who are the potential data recipients of such data,
- for how long personal data will be retained,
- the possibility for individuals to enforce erase data or prevents its processing and enforce such rights through Data Protection Authorities.

Most of this information should generally be already represented in the Privacy Notice for the drone operation.

DO In addition, where requested, drone operators and pilots should provide individuals with a copy of their personal information. This can be in the form of videos or still frames. Before sharing footage or images in which a person is captured, steps will be taken to remove the personal data of others captured.

Where a drone operator or pilot holds personal data and an individual makes a request for a right to access to the data to the client of the drone services, the drone operator / pilot should support the client in complying with such request, as soon as the operator or pilot is informed of it.

Right to data portability

Where a drone operation processes personal data on the basis of individual consent or a legal contract with an individual, individuals have the right to data portability,[25] which should be respected by drone operators and pilots.

This right allows individuals to request that:

- they receive copies of their data in a commonly-used and structured format, and/or
- their data is directly transferred to another data controller of their choice.

Right to object

Individuals have the right to object to their personal data being processed and permanently prevent it, if the processing is based Article 6(1)(e) GDPR (processing in the public interest or in the exercise of official authority) or Article 6(1)(f) GDPR (processing for a legitimate interest, such as direct marketing).[26] Generally, the right to object is guaranteed to individuals by the GDPR in a limited set of situations, where interference with their privacy and data protection may be disproportionate. Such circumstances are more detailed in Article 21 GDPR.

DO Given that personal data is, in most cases, not necessary for the achievement of the purposes of a drone operation, responsible drone operators or pilots, should seek to always comply with the request of individuals not to have their personal data processed.

[25] Article 20 GDPR.
[26] Article 21 GDPR.

TIP As the personal data of an individual is not easily separated from the totality of a recording made by a drone, e.g. a video or image, to comply with this right, drone operators and pilots should do the following:

- Where individuals have requested that they are not captured by a drone, and as far as possible, drone operators should plan flight paths that respect such a request. To achieve this, individuals should be clearly informed of when and where the drone will fly, enabling them to prevent being captured as well.

- Where individuals have requested that they are not captured by a drone, however, it is not possible to complete the purpose of the drone flight without doing so and there is a legal basis for the operation, their personal data should be anonymised or erased as soon as the drone flight is completed. Individuals should be informed of this, as well as of the time and flight path of the drone.

- Where individuals have requested that their images, once captured, are not processed, the drone operator should take steps to anonymise or erase their personal data as soon as possible.

Right to erasure

DO People have the right to request that their personal data is erased.[27] As with the right to object and given the fact that personal data collection by drones often takes place without an individual's awareness or consent and is an unnecessary side product of a drone flight, drone operators and pilots should seek to always respect data subjects' requests to have their personal data erased by completely and securely erasing all copies of relevant data recorded by drone or anonymising such data by blurring or hiding parts of it.

In exceptional circumstances, drone operators and pilots may be allowed to retain such data despite the request of individuals, such as for the exercise of freedom of expression and information, as with journalistic uses of drones. Drone operators and pilots may consult Article 17 GDPR for such possibilities.

Right to restriction of processing

DO In a limited set of circumstances, individuals have the right to request that the processing of their personal data is temporarily restricted, though the data is not erased.[28] Drone operators and pilots should comply with this right within its scope, pursuant Article 18 GDPR.

TIP To ensure compliance with this right at a reasonable burden for drone pilots and operators and, considering the nature of visual data collected through drones, drone operators could consider acting in the following way:

[27] Article 17 GDPR.
[28] Article 18 GDPR.

- creating a copy of the drone data and relevant visual and other information, featuring the personal data, subject of the rights request;
- anonymising or erasing the relevant personal data from one copy of the data. In this way, working with this copy will restrict the further processing of the personal data;
- retaining an unaltered copy of the relevant personal data for as long as it is necessary. This will depend on the reasons for the restriction of processing in the first place.

Put policies in place to comply with rights of individuals in practice

DO Where drone operators act as data controllers, they will be responsible for guaranteeing that the rights of individuals are respected. To ensure this, drone operators should create clear policies and procedures to guide the efficient, accessible and swift exercise of rights by individuals. Such procedures should be easy and quick from the point of view of individuals, whose personal data is being processed.

Individuals should in general be able to make rights requests free of change. In exceptional circumstances, drone operators may be allowed to charge small fees for such requests to cover rising administrative costs or where data subjects are acting excessively.

TIP Streamlined and comprehensive internal procedures for responding to data subject rights requests should include mechanisms to:

- Handle and document both verbal and written requests by individuals;
- Verify the identity of individuals claiming rights by requesting a proportionate amount of information, e.g. an image of their ID with unnecessary personal information deleted; [29]
- Identify what additional information may be requested by data subjects, e.g. a timeframe and location when individuals believe they were captured by a drone;
- Decide when a rights request should be complied with and when not;
- Prepare answers to individuals, including what information and in what form should be shared with them;
- Set a timeline to respond to individual requests within a month of receiving them;
- Identify when other data recipients should be informed of data subject rights requests and decisions made in response to them.

Communicate data subject rights requests to partners

Acting as a data controller or a joint controller

Where a drone operator is a data controller and they receive a data subject rights request, the drone operator should follow internal procedures or otherwise take steps to ensure that individual rights request is handled in accordance with the GDPR.

[29] Information Commissioner's Office, "Guide to the General Data Protection Regulation GDPR: Individual rights". https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

Where a drone operator is a joint controller together with a client who has hired their services and where the individual rights request received falls within the scope of data protection responsibilities of the drone operator, as laid down in the Joint Controller Agreement, the drone operator should follow internal procedures or otherwise take steps to ensure that the individual rights request is handled in accordance with the GDPR.

Where a drone operator / pilot acts as a data controller or joint controller and they have decided to comply with a data subject rights request for the erasure of personal data or an exercise of the right to object or restrict processing, they should immediately inform any other recipients of the personal data of this.

Acting as a data processor

Where the drone operator is a data processor, they should inform the relevant data controller of the individual rights request and refer the decision of handling the request to the controller. Once the controller has taken a decision, the drone operator should follow their instructions.

Where a drone operator / pilot acts as a data processor or joint controller and they are informed by their data controller or a joint data controller of a data subject right requests for the erasure or an objection to the processing of personal data that is complied with, they should take steps to comply with such a request and support the data controller in doing so. To this end, a drone operator / pilot may have to provide any data necessary to the data controller or the joint controller in a timely and efficient manner and, in the case of an exercise of the right to object, to erase or to restrict processing, should immediately cease to process such data and comply with further instructions by the controller.

4.4 Treat data diligently

4.4.1 Retain and use data within the limits of the law

Retain only what is necessary and anonymise as much as possible

DO

After a drone operation, drone operators and pilots should retain only personal data which is necessary for the purpose of the drone operation and which they have a legal basis to hold. Personal data should not be maintained in a manner which allows the identification of individuals for longer than necessary, pursuant to Article 5(1)(e) GDPR.

Data should be minimised by being securely erased or anonymised (e.g. through blurring faces, car and house numbers, etc.) as soon as it is no longer necessary or when it becomes excessive.[30] All copies of personal data, e.g. on local storage drives, on drone equipment or cloud computing platforms, should be erased or anonymised once no longer necessary.

[30] You can read more about anonymising data safely here: Information Commissioner's Office, Anonymisation: managing data protection risk code of practice, November 2012. https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Where drone operators and pilots wish to retain data which features personal data, markers, images and other details related to individuals should be anonymised.

Where drone operators are under a legal obligation to archive data collected, such data should not be processed and securely erased once the retention period is over.

TIP Drone operators should establish procedures to minimise the personal data held, processed and stored. This could include:

- regular data audits and reviews to identify unnecessary data;
- time-limits for data retention from completed drone operations or guidelines how to set such time-limits.

TIP Where appropriate, drone operators should explore and use technical features and software which support responsible data retention practices. Such features could include:

- automatic anonymisation techniques;
- automatic data erasure from drone equipment after every drone operation/flight,
- custom-set reminders for discarding older data.

Process personal data only for its intended purpose and compatible purposes

DON'T Drone operators and pilots should not extend or change the purpose of their drone operation or the processing of personal data without prior consideration of their legal requirements, including the requirement to inform individuals and act transparently. Once personal data has been collected, drone operators and pilots should only process it for: [31]

- the original purpose for which it was collected;
- a new purpose that is *compatible* with the initial one. A compatible purpose is connected, related to the original one, and it could be expected by the individuals on the ground.

If these conditions are not met, but a drone operator or pilot wishes to process personal data further, this would be processing for an *incompatible* purpose – a purpose which is very different, unexpected or can have unjustified impact on individual. Processing for an incompatible purpose is only allowed where:

- a new legal basis for such processing is established *and*
- individuals concerned are informed of this new purpose and their rights, including their right to object to such processing. [32]

[31] Information Commissioner's Office, "Guide to the General Data Protection Regulation GDPR: Lawful basis for processing". https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/.
[32] Recital 50, GDPR.

4.4.2 Handle data securely

Treat data securely

DO Drone operators and pilots should ensure that data is processed, stored, transferred and erased securely. Personal data should be protected from unauthorised or unlawful processing and against accidental loss, destruction, or damage[33] in accordance with Article 32 GDPR.

Technical and organisational security measures should be implemented to protect personal data captured during drone operations. This protection should apply to the entirety of the personal data lifecycle – from its collection, to its anonymisation or destruction.

The cost and protection offered by the security measures chosen should be proportionate to the likelihood of a data breach and the impact on individuals in case of a data breach.[34] In cases where large amounts of personal data or where special categories of personal data is collected, security measures of higher cost and quality should be implemented.

Technical measures to secure data

DO Appropriate and proportionate technical measures should be implemented to ensure the security of personal data collected and stored. Equipment possessing the necessary technical capabilities and settings should be chosen, as proportionate to the risks likely to arise in the context of the drone operation.

TIP Personal data and privacy could be protected while collected, stored and transmitted. Measures to protect personal data include:

- encryption of data
- access controls limiting unauthorised access to data
- automated log of user access to personal data and processing carried out on personal data stored
- equipment and software, compliant with security standards and certification schemes

Security considerations should cover:

- drone equipment and flight controls during flight
- drone equipment after landing
- transmission of personal data between the drone equipment and pilot station
- transfer of personal data between different storage devices
- storage of personal data on drone equipment, on local drives, servers and cloud computing services

[33] Article 5(1)(f) GDPR.
[34] Article 32(1) GDPR.

Drone equipment that ensures a secure and safe flight should always be used.

Organisational measures to secure data

DO Data security should be ensured within the internal procedures and practices of a company, as well as within the choice of devices and equipment used. Employees should be trained to consider information security and data privacy when working with technology, when transferring, accessing or erasing data.

Access to personal data should be limited to authorised persons who need access to carry out their functions. Procedures should be laid down to provide authorisation for access to personal data collected by specific drone operations.

DO Specific data security tasks should be delegated to those responsible with handling personal data.

Prepare against and minimise the impact of a data breach:

To minimise against the impact of a data breach, drone operators should incorporate appropriate technical and organisational safeguards to limit the data accessed during a breach, the type of data accessed and the duration of the breach.

DO Clear policies and procedures should be implemented to guide how data breaches are handled. Employees should be trained how to quickly and effectively react if data breaches occur.

DO Regular testing and reviews of security measures should take place to ensure security measures remain adequate and appropriate for the relevant drone operations.

Notify a data breach to your partners and Data Protection Authorities

DO Where a drone operator suffers a data breach that impacts the personal data they hold, the drone operator needs to take steps to inform any data controllers or joint data controllers, as well as the responsible authorities of the breach**.** The drone operator should determine who to inform.

- Where the drone operator acts as a data controller or a joint controller, they should notify a data breach to the responsible Data Protection Authority within 72 hours of discovering the breach, unless the breach is unlikely to result in risks to the rights and freedoms of the data subjects affected. Where a drone operator makes such a finding, they should document it and its rationale.[35]

- Where the drone operator acts as a drone processor, they should, without undue delay, inform their data controller of the breach.

[35] Recital 85 GDPR.

- Where the drone operator acts as a joint controller, they should also take steps to immediately notify their joint controllers of the breach.

The content of a notification of a data breach to a Data Protection Authority should be in accordance with the requirements of Article 33(3) GDPR and include, at least:[36]

- a description of the nature of the breach, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of data records (i.e. footage and data recordings) concerned;
- name and contact details of an appointed DPO or another contact point where further information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to be taken by the data controller to address the breach, including, where appropriate (and possible), measures to mitigate its possible adverse effects.

TIP A data breach notification to the competent supervisory authority is not necessary where it is unlikely to raise any risk for the data subjects impacted. This could be the case where:

- data has been anonymised;
- no detailed personal data is captured, such as a combination of a face and transportation vehicle used, home address or place of employment.

Notify a data breach to the individuals concerned

DO Where a drone operator suffers a data breach that is likely to result in a high risk to the rights and freedoms of the individuals concerned, the data controller should inform them without undue delay of the data breach.

Such notice should be in plain language and include similar information as a notification to the responsible Data Protection Authority (see above) with the exception of a description of the nature of the breach.[37]

TIP Since the individuals are often unknown to the drone operator, a public communication or similar measure to inform impacted individuals in an equally effective manner may be mandatory according to Article 34(3)(c) GDPR.

[36] Article 33(3) GDPR.
[37] Article 34(2) GDPR.

4.4.3 Share and move data responsibly[38]

A legal framework for sharing personal data

Drone professionals may be required to share data they collect with external parties, e.g. clients or data processors. Regardless of whether a drone operator is acting as a data controller, joint controller or a data processor, the data sharing process should be formalised in a. agreement setting out the rights and obligations with regard to the sharing of personal data to ensure personal data is handled in compliance with the GDPR and a high level of data security is ensured throughout by any data recipients.

DO Data recipients should be responsible for ensuring that personal data in their possession is handled in compliance with the GDPR.

TIP As good practice, the agreement should include:[39]

- the identities of the data sharing partners, potential recipients and circumstances under which data will be shared;
- the purpose(s) and use of data to be shared;
- the data to be shared – categories, type amount;
- the categories of individuals data belong to;
- the nature and duration of processing;
- the time and manner for it to be shared – as a regular occurrence or a one-time event;
- the way in which data will be shared, including how to guarantee the accuracy and security of the data;
- how long data will be retained for by the recipients;
- the rights of individuals and the procedures to ensure them;
- sanctions for failures to comply with the agreement.

DO Any sharing arrangements and data recipients should be reflected in the Privacy Notice of the drone operation.

A responsible data processor

DO Data controllers are responsible for the data handling practices of data processors they engage, and data processors are responsible for data sub-processors. The choice of data processors or sub-processors is important for ensuring personal data is handled in compliance with the GDPR

Engaging a processor

[38] You can read more about some best practices in sharing personal data with others here: Information Commissioner's Office, Data sharing code of practice, May 2011. https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf .

[39] FRA Handbook, p. 109; Information Commissioner's Office, Data sharing code of practice, May 2011, p. 26. https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf.

Where a drone operator or pilot wishes to engage a data processor, e.g. cloud services for data storage or processing, due care should be taken to ensure that a data processor handles any personal data shared in compliance with the GDPR and in a secure manner. A way to do this is by either examining the standard Terms & Conditions of the cloud service or, where there are none, concluding a Data Processing Agreement with the chosen data processor.

A Data Processing Agreement with a data processor (or their Terms & Conditions) should, in addition to formalising the data processing, meet the requirements of Article 28(3) GDPR and ensure that:

- the data processor is to act only and exclusively on instructions by the data controller and the processing which the processor is to carry out on behalf of the instructor;
- the data processor is to protect privacy and comply with data protection law – the GDPR specifically, e.g. by having their own privacy policy in place and **ensuring** the security of personal data in their possession;
- the data processor is liable for their own mistakes and failures;
- they implement equal precautions to protect personal data and privacy if they engage sub-processors of their own.

Engaging sub-processors

Where a drone operator acts as a data processor and wishes to engage sub-processors, they should inform the data controller whose instructions they follow of the choice, change or addition of a data sub-processor. The data controller should have the opportunity to object to the sub-processor and the data processor should comply with the instructions of the data controller.

DON'T Data processors or sub-processors who have a poor reputation with regard to data security or data privacy and/ or that have not obtained any visible data security credentials should be avoided. The same applies, if the standard Terms and Conditions of a data processors do not meet the requirements of Article 28(3) GDPR.

Minimise personal data shared

DO Share the minimum amount of personal data with external parties necessary for the purpose of the drone operation.

Where achieving the purpose does not require the sharing of personal data, only anonymised data should be shared.

Where the purpose of data collection and the drone operation does not allow for data to be anonymised, any unnecessary personal data collected should be discarded and only the minimum amount of data necessary for the purpose of the operation should be shared.

TIP Drone operators should discuss with clients and other data recipients, before sharing data with them, what the form, quality and quantity of data shared should be. This should be reflected in the Data Processing Agreement.

Transfer personal data to third countries with legal safeguards

DO When a drone operator plans to share personal data with parties or international organisations based outside of the EU and the EEA, special precautions are necessary and legally required to ensure personal data is protected beyond the borders of the EEA.

One of the following conditions must be fulfilled to ensure data protection standards are met where personal data is transferred outside the EU and the EEA:

- personal data is transferred to countries which have been declared to have an adequate level of protection by the European Commission in accordance with Article 45 GDPR;
- standard data protection clauses approved by the European Commission[40] or new standard clauses adopted by supervisory authorities and approved by the Commission in accordance with Article 93(2) GDPR are used;
- personal data is transferred to a country where there are binding rules, agreed between public authorities;
- the data recipient has made enforceable commitments to and complies with an approved Code of Conduct or a certification scheme in accordance with Articles 40 and 42 GDPR;
- binding corporate rules are employed in accordance with Article 47 GDPR, where personal data is transferred to another company in the same corporate group as the drone operator.

Share data with authorities, when required

DO Where drone pilots / operators are under a legal obligation to share data collected with authorities and public bodies, they should comply with their legal obligations.

Where drone pilots / operators act as data processors and a data controller is under a legal obligation to share data collected with authorities and public bodies, drone pilots / operators should support the data controller in complying with their legal obligation by providing any data necessary.

TIP Document any decisions to share data with public authorities and the rationale behind it.

[40] European Commission, "Model contracts for the transfer of personal data to third countries". https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

4.5 Ensure compliance with the GDPR in practice

4.5.1 Comply with legal responsibilities in practice

Document your activities

DO To establish compliance with the law and ensure accountability in accordance with Article 30(2) GDPR, drone operators / pilots carrying out drone operations where personal data is captured should maintain records about the following details concerning their activities and their processing of personal data. Record-keeping should cover the entire lifecycle of personal data, from its collection until tis permanent erasure or anonymisation.

Grounds and nature of processing:

- the legal basis of drone operations where personal data is processed and rationale for such decision, as well as documentary proof of compliance with the legal basis;
- the purposes of data collection and processing;
- the categories of processing of personal data carried out by the drone pilot / operator – from the data's collection until its final deletion or anonymisation;
- the retention period of personal data.

Security of processing:

- a general description of technical and organisational security measures;
- any data breaches suffered, their facts, effects and remedial actions taken; [41]
- confidentiality obligations or requirements of involved staff.

Compliance instruments:

- adherence to any relevant data protection codes of conduct or certification schemes.

Sharing of personal data:

- the legal relationships with bodies with whom personal data is shared (e.g. Data Processing Agreements);
- any decisions made to share personal data with external bodies, e.g. public authorities and the rationale behind it.

Where applicable, drone operators / pilots should also document any transfers of personal data to third countries outside the EU or the EEA and basis on which such transfers took place, e.g. what suitable legal safeguards have been implemented.

All records should be provided to supervisory authorities upon request.

Additional information to be documented

[41] Article 33(5) GDPR, Recital 85 GDPR.

TIP You may not be legally required to document some pieces of information, but it may, nevertheless, be best practice for you to do so and it is recommended that you do so.

- Where you decide not to notify data breaches, document decisions about whether data breaches raise risks for individuals and the rationale for such decisions;
- Where you make decisions regarding data subject requests to exercise their rights, document the decisions and the rationale behind it;
- As a security precaution, maintain an up-to-date list of all staff with access to personal data and all data processors or sub-processors used.

Where a drone operator / pilot acts as a data processor, they have to assist the data controller in maintaining adequate records for the controller's data protection compliance. Thus, the data processor may provide its own records related to the respective data processing to the data controller upon request. However, only personal data which is required by the data controller should be provided.

Put in place internal privacy policies and procedures

DO To facilitate the day-to-day management of privacy and data protection issues, drone operators should create internal procedures for their organisation which can guide employees in complying with requirements of:

- principles guiding drone flight planning and execution, in particular with a view of minimising drone flight over or near private and sensitive spaces and minimising personal data captured and recorded;
- access to and treatment of collected data, including security measures;
- data retention and destruction;
- granting access to third parties;
- handling a data breach; and
- procedures to facilitate individuals exercising their data protection rights.

Policies should be regularly reviewed and updated to ensure their effectiveness.

Employee training

DO Drone pilots and members of the drone piloting team should be well-trained and aware of how to carry out drone flights in practice, minimising any interference with the rights and freedoms of uninvolved individuals on the ground. In particular, the drone operator should ensure that the piloting team is:

- familiar with and able to operate the drone equipment effectively in a way to minimise any personal data collected,
- aware of the flight area and context, as well as the pre-planned flight path,
- capable of providing further information regarding the drone operation to by-standers and able to refer them to the Privacy Notice for the drone operation.

Drone pilots and other employees with access to personal data collected after a drone operation should also be trained and well-aware of data management and security policies and practices adopted by the drone operator.

TIP An employee may be delegated, who can oversee compliance with data protection, safety and security procedures.

Be prepared if your activities are a high-risk for individuals

DO If drone operations are liable to pose a high risk to the rights of individuals, drone operators and pilots should carry out a Data Protection Impact Assessment (DPIA) pursuant to Article 35 GDPR. A drone operation is liable to raise high risks for individuals where sensitive information about individuals is regularly processed or large amounts of personal data are collected.

The safeguards and mitigating measures identified within a DPIA in response to data protection risks should form a part of any drone operation planning and be implemented in practice. Where a DPIA is not followed in practice, drone operators should update the DPIA to correspond to the drone operation.

TIP National Data Protection Authorities have issued and will issue whitelists on their websites, clarifying when they deem a DPIA to be necessary. Please take a look at the website of your competent Data Protection Authority for the latest guidance available.

DO If a drone operator or pilot carries out drone operations, which result in the regular processing of special categories of personal data pursuant to Articles 9 and 10 GDPR or if drone operations are likely to involve the regular and systematic monitoring of individuals on a large scale, they should designate a Data Protection Officer (DPO) in accordance with Article 37 GDPR, who should support the operator's compliance with the requirements of the GDPR.

Implement this Code in practice

TIP The benefit of privacy and data protection will not be achieved until you implement these values in your day-to-day operations. Some concrete steps which you should take to make this Code effective include:

- carrying out a data audit, mapping data flows and data procedures against your legal requirements to be aware of your business' data and how to respect privacy and data protection within it;
- developing coherent and detailed internal procedures and policies to clearly lay out the standard behaviour expected of employees;
- carry out trainings to introduce employees to the Policies and refresh their knowledge;
- demonstrating support by management personnel to foster a privacy-aware organisational culture.

4.5.2 *Enforce legal responsibilities in practice*

Designated monitoring body[42]

When this Code is being reviewed by industry representatives, looking to submit the Code for legal recognition and approval by national Data Protection Authorities pursuant to Article 40 GDPR, industry members should designate a monitoring body to oversee the compliance of subscribing parties with this Code of Conduct, which monitoring body should comply with the requirements of Article 41 GDPR. Moreover, such a monitoring body should have sufficient understanding of privacy and data protection law, as well as drone operation and piloting to ensure a useful review of the implementation of the Code.

Powers of monitoring body[43]

The designated monitoring body, tasked with overseeing and ensuring the compliance of subscribing parties with the Code of Conduct, may, at any time, request records of processing activities by drone pilots and operators in order to inspect their compliance against the requirements of the Code.

Where the designated monitoring body wishes and if this does not pose any risk to the safety of the drone operation, a representative of the body may be present during a drone flight(s) and oversee their practical execution.

Where the designated monitoring body wishes and if this does not raise particular privacy concerns on the part of the operator and/or pilot, a representative of the body may inspect the premises of the drone operator and/or pilot and the manner in which data is handled in practice.

Drone pilots and operators should respect such authority and cooperate with the designated monitoring body in a timely manner.

Respect for powers of Data Protection Authorities

Drone operators and pilots should fully cooperate with Data Protection Authorities, whenever so requested.

5 CONCLUSION

The goal of this Code of Conduct has been to inform drone operators and pilots of the practical steps necessary when operating a drone for professional (e.g. commercial) purposes in order to minimise impacts on the privacy and personal data of individuals

[42] Article 41(1) GDPR.
[43] Article 40(4) GDPR.

on the ground. It is up to drone operators and pilots to use this resource, together with the other DroneRules.eu information resources, to ensure responsible drone activities and establish a culture of privacy awareness and data protection among the drone industry in Europe.

In cases where there are any questions or concerns, drone pilots and operators are encouraged to consult a legal professional or your national Data Protection Authority.