



# PRIVACY-BY-DESIGN GUIDE

A DroneRules.eu PRO resource for drone  
manufacturers

## Table of Contents

|  |           |
|--|-----------|
| <b>WHAT IS THIS PRIVACY BY DESIGN GUIDE?.....</b>                                    | <b>2</b>  |
| <b>7 PRINCIPLES OF PRIVACY BY DESIGN IN THE CONTEXT OF DRONE MANUFACTURING .....</b> | <b>4</b>  |
| 1.    PROACTIVE, NOT REACTIVE .....  | 4         |
| 2.    PRIVACY AS THE DEFAULT SETTING .....   | 5         |
| 3.    PRIVACY EMBEDDED INTO DESIGN .....   | 5         |
| 4.    FULL FUNCTIONALITY.....  | 5         |
| 5.    END-TO-END SECURITY .....  | 5         |
| 6.    VISIBILITY / TRANSPARENCY .....  | 6         |
| 7.    RESPECT FOR PEOPLE / USER-CENTRIC APPROACH .....                               | 6         |
| <b>FUTURE REGULATION AND PRIVACY-ENHANCING DRONE DESIGN .....</b>                    | <b>8</b>  |
| <b>PRIVACY RISKS AND SAFEGUARDS IN DRONE MANUFACTURING .....</b>                     | <b>10</b> |
| DRONE DESIGN AND PRIVACY .....   | 10        |
| <i>Colour and logos</i> .....  | 10        |
| <i>Number of rotor blades</i> .....  | 11        |
| <i>Size of drones</i> .....  | 11        |
| <i>Sound of drones</i> .....   | 12        |
| <i>Location of camera</i> .....  | 12        |
| <i>Lack of payload feedback</i> .....  | 12        |
| DRONE HARDWARE (PAYLOADS AND CAPABILITIES) AND PRIVACY .....                         | 13        |
| <i>Proportionality in drone design</i> .....   | 13        |
| <i>Payload and sensor control</i> .....  | 14        |
| <i>Communication capabilities</i> .....  | 15        |
| DRONE PRIVACY-ENHANCING SOFTWARE FEATURES .....                                      | 15        |
| <i>Geo-awareness capabilities</i> .....  | 15        |
| <i>Electronic identification</i> .....   | 17        |
| <i>Logs of flights and activities</i> .....  | 18        |
| <i>Automated data minimisation</i> .....   | 18        |
| <i>Drone digital security and data protection</i> .....                              | 19        |
| DRONE PACKAGING AND PRIVACY.....   | 22        |
| <i>Provide drone pilots and operators with information</i> .....                     | 22        |
| <i>Labelling of drone</i> .....  | 23        |
| <b>HOW TO APPLY THESE PRINCIPLES IN PRACTICE .....</b>                               | <b>25</b> |
| <b>CONCLUSION .....</b>  | <b>28</b> |
| <b>ANNEX I DATA PROTECTION AND PRIVACY LEAFLET .....</b>                             | <b>29</b> |
| <b>ANNEX II SECURITY AND SAFETY LEAFLET .....</b>                                    | <b>30</b> |
| <b>ANNEX III INSURANCE LEAFLET .....</b>   | <b>31</b> |

## What is this privacy by design guide?

This privacy by design guide is aimed at drone manufacturers and it is intended to help them incorporate privacy into the process of designing and building drones. The guide:

- will introduce you to the fundamental privacy by design principles,
- will guide you through applying them in practice by providing you with a questionnaire to help you assess privacy risks and identify appropriate safeguards, and
- will provide you with an overview of the privacy risks which different drone features can give rise to, readily proposing potential solutions.

Privacy by design is important because the General Data Protection Regulation (GDPR) requires organisations that process personal data to apply the principles of data protection by design and by default (e.g. drone pilots and operators). These principles aim to ensure that data protection and privacy considerations play a role in the design and development of new technologies, processes and flight plans from the very beginning and that they ensure that as little personal data is processed by default.

Following this guide and its recommendations can help you incorporate privacy into the products you create from the design and development stage. Privacy risks can arise in relation to various aspects of a drone's design and operation, from its data capturing and processing activities,<sup>1</sup> to its operation<sup>2</sup> and even its appearance.<sup>3</sup> For these reasons, privacy by design has to be a leading step of the design and manufacture of drones.<sup>4</sup> This is particularly important with drones. Thanks to their size, agility and diverse capabilities, drones could potentially collect large quantities of personal data with very little transparency.

In the GDPR, the requirements of data protection by design and by default apply to data controllers – the people or entities who determine the purposes and means of the processing of personal data. In the context of drone operations, these will most likely be the drone operators (or, depending on their contractual arrangements – their clients) and drone pilots, but this will be a case by case determination. Even if these obligations do not apply directly to the manufacturer of a drone itself, they apply to drone operators when choosing their equipment prior to the collection of personal data. Implementing data protection principles and the requirements of privacy by design and by default as a manufacturer is therefore required in order to enable your customers to lawfully operate your drone. Thus, it could give you a significant competitive advantage and help distinguish your products from those of your competitors by supporting the data protection compliance of your customers.

---

<sup>1</sup> Anne Gerdes, and Privacy Issues, Information, Technology and Innovation Research Group at University of Southern Denmark, Drones, 2017, presentation slides. [http://infotechinno.sdu.dk/pdfs/Drones%20and%20privacy%20SDU\\_042418.pdf](http://infotechinno.sdu.dk/pdfs/Drones%20and%20privacy%20SDU_042418.pdf)

<sup>2</sup> Altawy Riham and Amr. M. Youssef, "Security, Privacy, and Safety Aspects of Civilian Drones: A Survey", *ACM Transactions on Cyber-Physical Systems*, Vol. 1, Issue 2, Article 7, November 2016, 25 pages. <https://users.encs.concordia.ca/~youssef/Publications/Papers/Drone-Survey.pdf>.

<sup>3</sup> Chang, Victoria, Pramod Chundury, Marshini Chetty, "'Spiders in the Sky': User Perceptions of Drones, Privacy, and Security", *CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, May 06-11, 2017, Denver, CO., USA, pp. 6765 – 6776. [https://hci.princeton.edu/wp-content/uploads/sites/459/2017/01/CHI2017\\_CameraReady.pdf](https://hci.princeton.edu/wp-content/uploads/sites/459/2017/01/CHI2017_CameraReady.pdf)

<sup>4</sup> Cavoukian, Ann, "Privacy and Drones: Unmanned Aerial Vehicles", Information and Privacy Commissioner, Ontario, Canada, August 2012, p. 4. <https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-drones.pdf>.

In addition to improving the quality and marketability of your drone, certain privacy-enhancing features may soon become legally mandated for drones on the European market. European legislators are currently discussing certain technical requirements for drones, some of which have a direct bearing on the privacy impacts of drones. Once these requirements become law, you will be legally obligated to comply with them if you wish to sell your drones in Europe.

Finally, parts of this guide are also relevant for producers of sensors (fixed or modular payloads) and software, used in the manufacture of drones. The parts and pieces of drones often come from different sources and are only assembled together by a single manufacturer or – in case of modular payloads – is attached to a drone even by the drone operator. It is just as important to ensure that software and sensors used in the make of a drone incorporate privacy by design wherever possible.



We suggest that you consult this guide alongside other DroneRules PRO resources available via the website, as well as any relevant updates to legislation that may be applicable to your drone manufacturing activities, especially when your drones may be used for processing personal data.

## 7 principles of privacy by design in the context of drone manufacturing

There are seven foundational principles of privacy by design that help explain what this concept means in practice.<sup>5</sup> This guide will introduce you to some specific risks and safeguards you should consider as a way of applying privacy by design to your work. However, these principles constitute overarching guidance about your obligations that can be used to develop specific privacy by design measures relevant to the use and operations of your drone. We have included a brief description of the overarching principles of privacy by design below and how they could apply to drone manufacturing.<sup>6</sup>

### 1. Proactive, not reactive

Privacy by design encourages a proactive approach. Rather than waiting for a risk to materialise, as a drone manufacturer, you should act preventively and consider how to best protect privacy by implementing additional features and safeguards in the design and build of your drone. By considering privacy enhancing technologies which can be applied to the drones you manufacture, you are not only making your products more competitive, but you may also be effectively preventing privacy infringements from taking place.

Key examples of drone features which could help achieve this principle include:

- Providing the drone with geo-fencing and other limitation sensing technology;
- Equipping the drone with software controls which allow users to easily tailor the sensors used and the data quality captured for their particular operation;
- Incorporating software into your drone or functionalities in the software to control your drone that allows users to activate or deactivate drone sensors and/or payloads to be engaged for a particular flight, thus achieving modularity in practice;
- Providing software controls for users to be able to trigger or prevent data recording when desired during a flight;
- Placing access controls and encryption on the drone itself and data stored on it, as well as on the ground control system through which it is operated;
- Implementing additional software features which minimise data by:
  - Limiting data collection, e.g. by turning off data collection when a drone strays from its predetermined flight path or allowing their easy turning on and off so that they function only when necessary,
  - Limiting data retention, e.g. by automatically erasing all data on the drone after it has been downloaded following a flight,
  - Automatically detecting human shapes and removing them through blanking, hiding or blurring them, thus anonymising personal data captured.
- Ensuring an overall high level of information and IT security in the drone's systems, thus protecting the drone and access to its data.

---

<sup>5</sup> Cavoukian, Ann, "Privacy by Design: The 7 Foundational Principles", Information and Privacy Commissioner, Ontario, Canada, January 2011. <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>.

<sup>6</sup> See Cavoukian *supra* n 4, p. 19.

## 2. Privacy as the default setting

The design and settings of drones, their payloads and the software they run should be geared towards ensuring privacy by default. As soon as a drone is unboxed, it should be programmed to be as privacy-protective as possible. This is similar to the principle of data protection by default which requires that the principle of data protection by design is respected by both manufacturers and operators and should apply to the entire lifecycle of a technology, including its design and manufacturing.<sup>7</sup> This will not only allow you to showcase the more advanced features of the drone but will also support users in complying with their obligations more easily.

By considering privacy and data protection during the design and manufacture of your drone products, the drone equipment, drone interface and programs, drone controls you produce should be as privacy-preserving as possible by default. Without the need for end-users to alter the drone's features or settings, the drone should, for example:

- comply with geo-fencing or other drone limitations it senses,
- require access controls, such as passwords, to limit access to data collected and to controls of the drone,
- encrypt data on the drone,
- collect the least amount of data by, among others, being equipped with software capabilities which can trigger the activation of data sensors and data collection capabilities only when a set of conditions are met (such as location, timing, flying within a predetermined area),
- store data for the least amount of time.

If users wish to change these settings, they would be able to, but they would have to specifically decide to do so and make a conscious decision to that effect.

## 3. Privacy embedded into design

Privacy considerations should be embedded into the design and architecture of drone systems and drone products. Privacy considerations should become part of the product and its functionality, rather than being added after the design has been completed. By systematically considering the potential privacy impact of your drone and its equipment and considering how it would likely be used, you will be able to decide what safeguards are appropriate to incorporate into the design of your drone, its payloads, software and interface.

## 4. Full functionality

Privacy by design should not come at the expense of your product's quality and functionality. Privacy by design can be incorporated in a way which enhances your product and does not interfere with its key features disproportionately. There should not be a choice between privacy and your product's functionality. Both can be achieved together, especially if privacy-protection is viewed as a further enhancement to drones.

## 5. End-to-end security

Privacy should be protected through security considerations incorporated throughout the entire process of functionality of drones. This means that security measures should cover the security of drones while on or off, while operating in the sky or landing on the ground. Security should

---

<sup>7</sup> Article 29 Data Protection Working Party, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 01673/15/EN WP 231, 16 June 2015, p. 14. (Called 'A29WP Opinion on Drones' below)

protect data throughout its entire lifecycle on the drone – from data collection through to storage either locally on the drone or after transmission to other programmes or devices, and finally to the secure erasure of the data. A special section relating to information and IT security in the context of drone manufacturing can be found in the section entitled “Cybersecurity throughout the drone’s systems” below.

## 6. Visibility / transparency

The principle of visibility and transparency seeks to ensure that all impacted stakeholders have a way to verify that privacy is respected by the technology or process being developed. In the context of drone operations, people on the ground should have sufficient transparency and visibility of the activities of the drone and the drone operator or pilot. In the context of drone manufacturing, this principle would require you to develop drones which are clearly visible, but also to provide detailed information to drone pilots or operators about your product and about how it can be used in a way to protect the privacy of people on the ground.

In the context of drones this could be applied in a number of ways:

- making drones noticeable and implementing design elements which can signal to people on the ground that the drone’s sensors are currently active and capturing data,
- making available information about the components, building parts and software features, part of the drone, which enhance privacy and how they operate,
- complying with audited security / privacy standards or codes of conduct and presenting the documents to support this,
- implementing features in the drone software to log and track commands given to the drone during operations, instances of access to data or data deletion,
- including a detailed user manual and leaflet in the packaging of the drone with:
  - information about privacy-preserving features of your particular drone, and
  - detailed information about different payloads and their advantages and disadvantages to support pilots and operators in choosing the best features they need;
- equipping the drone with capabilities and features allowing it to communicate and integrate with apps or platforms that are intended to provide information to the general public regarding ongoing or future operations taking place with a specific drone model or a selection of different models.

## 7. Respect for people / User-centric approach

Respect for the privacy of individuals should drive all your actions when implementing the privacy by design approach. By placing users and individuals in the centre of your activities and considering how to (1) best respect their privacy and (2) enable others, using your product, to respect their privacy. This can be done both by incorporating privacy-preserving features in your drone, as well as by making these features user-friendly and informing your customers how to deploy them.

On the one hand, this principle requires you to consider how to design and build your drone with features which make respecting people’s wishes easy to achieve. For example, geo-fencing capabilities in a drone could allow it to easily detect when it enters areas where it is not welcome and to quickly inform the drone pilot of that, enabling him to take remedial steps.

On the other hand, you should also consider users when building your drone. As a manufacturer, take care to make privacy-preserving features easy to understand and to use. This will make them much more likely to be utilised in practice and will help enhance the appeal of your product and the compliance of users of your drone.



## EU wide drone rules and privacy-enhancing design

European authorities have been working on regulating drones and making some privacy-enhancing features mandatory. The regulations that have been published on 11 June 2019 separate drones into different classes, determined by their size, lifting power and flight capabilities and will ascribe each class with relevant requirements. These regulations are:

- the Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for operation of unmanned aircraft<sup>8</sup> and its ANNEX<sup>9</sup> (following called ‘Commission Implementing Regulation’), and
- the Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems<sup>10</sup> (following called ‘Commission Delegated Regulation’).

The Commission Delegated Regulation provides information particularly on drones which will be used in operations from an ‘open category’. That means flights carried out:

- in the visual line of sight of a pilot or their team member,
- the unmanned aircraft has a maximum take-off mass of less than 25 kg
- within heights not exceeding 120m above the surface, except when overflying an obstacle (as defined in the Commission Implementing Regulation),
- and the drone is kept at a safe distance from people and does not fly over assemblies of people, and
- considering the risks involved, requires neither a prior authorisation by the competent authority, nor a declaration by the UAS operator before the operation takes place.

This regulation could impact the way you incorporate privacy into your work by placing requirements or limitations on drones and on the process of drone manufacturing. Moreover, some aspects of regulation can assist privacy by design by requiring that privacy-enhancing technologies be built into a drone.

The Commission Delegated Regulation separates drones into different classes, based on their size and maximum take-off mass. Each class (C0, C1, C2, C3, C4) has to comply with a different set of technical requirements. The fulfilment of these requirements will not only determine whether your drone can be sold on the European Union market but may also impact the way that drone operators and pilots utilise the drones in practice, e.g. whether or not they can use them in particular subcategories of ‘open’ drone operations.

In addition, different drone classes are subject to different technical requirements and obligations for features or equipment. Overarching requirements include specific obligations on safe design

---

<sup>8</sup> Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft ([https://eur-lex.europa.eu/eli/reg\\_impl/2019/947/oj](https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj)).

<sup>9</sup> Annex to the Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft ([https://eur-lex.europa.eu/eli/reg\\_impl/2019/947/oj](https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj)).

<sup>10</sup> Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>). For further information about the latest EASA legislative matters with regard to the ‘open’ category of operations, please see <https://www.easa.europa.eu/document-library/opinions/opinion-012018>.)

and manufacturing, as well as providing information to users about the safe and responsible use of drones. However, there are specific requirements regarding drone capabilities and information and IT security which differ for different classes. As we introduce different means of incorporating privacy by design into drones, we will highlight whenever these will become legal requirements in the future.

It is recommended that you use the legal obligations set out in the Commission Delegated Regulation on drones as a guidance for other drones you manufacture. Although the Commission Delegated Regulation applies only to drones intended for use in ‘open’ category flights, you should consider expanding many of these recommendations beyond what is legally required for the following reasons:

- Regardless of the category of drone operation, drone operators and pilots will carry certain privacy and data protection responsibilities pursuant to the GDPR that they will need to comply with. These may include the responsibility to inform people on the ground of their activities, how they can minimise the amount of data collected and retained, as well as to ensure the security of data collected. Drone features are extremely important in achieving this.
- Most operations near or over assemblies of people uninvolved in the drone flight will be ‘specific’ category operations. Precisely ‘specific’ category operations are more likely to raise significant privacy and data protection concerns. The Commission Implementing Regulation reiterates the responsibility of operators in ‘specific’ operations to have procedures (and equipment) in place to ensure compliance with data protection laws.<sup>11</sup>
- The Commission Implementing Regulation provides Member States of the EU with the power to restrict drone operation in certain geographical zones, including for privacy and data protection reasons. As part of this, Member States may require that drones be equipped with particular privacy-enhancing features in order to be allowed to operate in certain designated areas,<sup>12</sup> e.g. cities. How countries will decide to regulate this is yet to be seen.

For these reasons, it is recommended that you consider recommendations on incorporating privacy by design into all drones that you create, even those that are not intended for use in ‘open’ category operations and which are not yet subject to concrete privacy-enhancing regulation or draft regulation.

---

<sup>11</sup> UAS.SPEC.050 (1)(a)(iv), *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft* ([https://eur-lex.europa.eu/eli/reg\\_impl/2019/947/oj](https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj)).

<sup>12</sup> Article 15, *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft* ([https://eur-lex.europa.eu/eli/reg\\_impl/2019/947/oj](https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj)).

## Privacy risks and safeguards in drone manufacturing

In order to understand the interplay between drones and privacy, we will systematically highlight how different aspects of a drone could interfere with the privacy and personal data of individuals on the ground. Specifically, we have divided this section into three topics:

- (1) Drone design
- (2) Drone hardware
- (3) Drone software
- (4) Drone packaging

In each section, we will highlight the principles and requirements which drones could interfere with and propose specific safeguards and features which could be used to incorporate privacy considerations into the drone. Where certain privacy-relevant features are also discussed as legal requirements in the Commission Delegated Regulation, this will be highlighted.

The end goal is to provide you with the tools to create drones that support drone users to comply with their own privacy and data protection legal obligations and operate drones in a responsible manner.

### Drone design and privacy

The way a drone is designed can affect how it is perceived by individuals on the ground and what privacy and security concerns they experience. Key aspects of your drone that may make your drone less threatening include its

- form and drone guard,
- shape,
- sounds (wind),
- drone movements and recording capabilities.<sup>13</sup>

If individuals on the ground feel that your drone looks threatening on a psychological level, they are more likely to feel surveilled and uneasy. This could lead them to self-censure their activities (in what is known as a “chilling” effect)<sup>14</sup>, to actively seek out drone pilots and operators and prevent their operation or to implement their own measures to prevent drones from flying near them or their homes, for example by using anti-drone technology.

There are steps, however, which you could take to prevent individuals feeling uneasy around drones and perceiving them as unfriendly machines.

#### Colour and logos

Traditional monochrome dark colour designs can be perceived as being unfriendly and less trustworthy by people. In addition, lack of logos or other signs on the drone could make people uncomfortable because these do not easily allow attribution of the drone’s behaviour to a person

---

<sup>13</sup> See Chang *supra* n 3, pp. 7-9.

<sup>14</sup> Finn, Rachel L., David Wright, Laura Jacques, Paul De Hert, “Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations: Summary for Industry”, European Commission, Ref. Area(2015)322948- 27/01/2015, November 2017, p. 7.

or company or identify its controllers.<sup>15</sup> This undermines the transparency and accountability of those controlling the drone. Moreover, dull and camouflage colours, especially on small drones, could increase the risk of people on the ground not being aware of drones operating over them.

You can easily remedy these concerns by using brighter colours in your design, which would make drones appear both less threatening and will make your drone more visible from the ground. Brighter colours have also been associated with evoking more positive emotions in people.<sup>16</sup> Furthermore, in the future drones in the classes C1, C2 and C3 will be required to be equipped with lights for improving controllability, in some cases extending the requirement to both daylight and night time conditions.<sup>17</sup> Such lights could also significantly enhance the visibility and noticeability of drones.

In addition to this, you can place stickers with your logo and the drone’s serial number or other identification information for the particular drone on it, in a clearly visible but protected place. This will not only help inform drone users of the particular capabilities of their drone, but it may also make people feel safer by making them aware of those responsible for the operation.

#### Number of rotor blades

The number of rotors which a drone has could also impact the way it is perceived by individuals. The design of drones has been linked to looking intimidating, violent, militarily or like “spiders”.<sup>18</sup> This could suggest that drones with more than 4 rotors – pentacopters, sextacopters, and so on – could be perceived as more threatening. On the other hand, circular drones can be considered less threatening and friendlier by people.<sup>19</sup> Furthermore, having guards around rotor blades can also be used to “soften” the look of drones and make users feel safer.<sup>20</sup>

#### Size of drones

The Commission Delegated imposes requirements on different drone classes intended for use in ‘open’ category operations regarding their maximum take-off mass (MTOM) or power exerted during a collision. An overview of such requirements, as they stand in the Regulation, is presented below:

|                                | Class C0 | Class C1  | Class C2 | Class C3 | Class C4 |
|--------------------------------|----------|---|----------|----------|----------|
| <i>MTOM, including payload</i> | < 250 g  | < 900 g or, during an impact between the drone and a human head at terminal | < 4 kg   | < 25 kg  | < 25 kg  |

<sup>15</sup> See Chang, *supra* n 3, p. 7.

<sup>16</sup> Hemphill, Michael, “A Note on Adults’ Color-Emotion Associations”, *The Journal of Genetic Psychology*, Vol. 157, Issue 3, 1996, pp. 275-280.

<sup>17</sup> Part 2.16, Part 3.18, Part 4.14, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>18</sup> See Chang *supra* n 3, p. 7.

<sup>19</sup> *Ibid*, p. 11. Sung, Ja-Young, Lan Guo, Rebecca E. Grinter, Henrik I. Christensen, ““My Roomba is Rambo”: intimate home appliances” UbiComp ’07 Proceedings of the 9<sup>th</sup> International Conference on Ubiquitous Computing, Innsbruck, Austria, September 16-19, 2007, pp. 145-162.

<sup>20</sup> See Chang *supra* n 3, p. 8.

|  |  |  |  |  |  |
|--|--|--|--|--|--|
|  |  | velocity,<br>transmits<br>energy < 80J |  |  |  |
|--|--|--|--|--|--|

In addition to drone classification, however, different drone sizes can also evoke different responses and concerns from people on the ground. If drones are too large, people may feel uneasy because they feel they are unaware of what payload a large drone carries or conceals. On the other hand, if drones are too small, they may become less noticeable, and stealth-like. Moreover, small drones may be able to access previously restricted areas due to their size.<sup>21</sup>

It seems like there is no easy solution to this issue, since both extremes in sizes give rise to different concerns. Nevertheless, there are some mitigating steps you could take for both situations. For example, if you manufacture large drones, provide guidance and information along with it, instructing users not to utilise it in cases where a smaller drone could suffice. If you wish to build smaller drones due to their lightweight and lower likelihood of injuring people, use other means to make the drones noticeable, such as colourful designs, light or sound signals. Combine this with providing information about its usage and instruct users not to operate drones in a concealed manner. The topic of informing users will be further detailed when discussing drone packaging below.

#### Sound of drones

Some people report feeling threatened by the sound and wind produced by drones. Although a louder drone could be easier to notice for people on the ground, loud drones are not encouraged. They could cause nuisance to uninvolved persons and give rise to feelings of unease. Such considerations have been recognised in the Commission Delegated Regulation and the maximum sound power level exerted by drones, at the time of entry on the market, has been set at a 85 dB(A) for drones in classes C1 and C2.<sup>22</sup>

#### Location of camera

Individuals have also reported being uneasy around drones due to the fact that they are not aware where the camera is located or even whether the drone is equipped with a camera. Since drone cameras are small, they may not be easily noticeable. This could make it difficult for individuals on the ground to know whether the camera is pointed in their direction or not.<sup>23</sup> You can remedy this by making cameras clearly visible by, for example, drawing attention to them through bright colours surrounding a camera lens.

#### Lack of payload feedback

The lack of any external indication on the drone itself about whether payload sensors are operating and capturing information or lack of understanding in the general public how to interpret such signals can make people feel observed even if they are not.<sup>24</sup> People on the ground can feel vulnerable when there is a drone in their vicinity if they have no way of telling then the drone's payload is actively engaged, e.g. whether a camera is recording or not even turned on. Here, we refer to payload sensors which are intended to collect data to fulfil the purpose of the drone flight

<sup>21</sup> See Chang *supra* n 3, p. 7.

<sup>22</sup> Part 15, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>23</sup> See Chang *supra* n 3, pp. 8-9.

<sup>24</sup> See Chang *supra* n 3, p. 9.

rather than simply sensors that are required to operate to ensure a safe and stable drone flight, such as gyro stabilisers.

You could mitigate this situation by incorporating a visual signal to let people around the drone that its sensors are engaged and capturing data. This could include a blinking light of a single or changing colour. Include guidance in the drone’s information leaflet on how drone pilots and operators can utilise these feedback sensors and advising them to disseminate information to individuals in the vicinity about this function and its meaning.

## Drone hardware (payloads and capabilities) and privacy

Drone payloads which include sensors and allow capturing data could give rise to privacy concerns among individuals on the ground. By capturing data, such as images, sound, geolocation and others, a drone could interfere with the privacy of individuals on the ground, especially if the captured data allows the identification of people (which in such case qualifies as the collection of personal data in terms of the GDPR).<sup>25</sup> Blurring of faces of people is not always a guaranteed way to prevent such identification in contexts which contain other details, such as house or car numbers. Therefore, it is recommended that you, as a manufacturer, consider what kind of hardware features and capabilities a drone should be equipped with.

### Proportionality in drone design

Different drone payloads and capabilities can give rise to different privacy concerns, depending on the kind of information they capture. A combination of these payloads or capabilities could especially lead to potential privacy risks materialising, e.g. a combination of images or videos captured with the precise location and time could more easily intrude into the privacy of people captured since it could allow the tracking of people’s whereabouts and activities. A brief illustration of this is available in the table below.

| <b>Payload / Capability</b>                                   | <b>Potential privacy impacts</b>  |
|---|---|
| <b>Zoom camera</b>  |   |
| <b>Thermal / infrared camera</b>                              | Bodily privacy  |
| <b>Multispectral NDVI camera</b>                              | Privacy of data and image   |
| <b>High resolution camera</b>                                 | Privacy of behaviour and action   |
| <b>LIDAR sensors (lasers)</b>                                 | Privacy of association  |
| <b>Facial recognition capabilities</b>                        | Privacy of thoughts and feelings ( <i>depending on context</i> )                        |
| <b>Other image capture tools</b>                              |   |
| <b>First-person view capability</b>                           | Dehumanisation of the surveilled and lack of accountability of drone operator / pilot   |
| <b>Extended range and endurance</b>                           |   |
|   | Privacy of personal communication   |
| <b>Directional microphone</b>                                 | Privacy of thoughts and feelings  |
|   | Privacy of behaviour and action   |
|   | Privacy of association  |
| <b>Galileo, GPS or other geo-location sensors</b>             | Privacy of location and space   |
| <b>Automatic number plate recognition (ANPR) capabilities</b> | Privacy of location and space ( <i>when applied to car plate numbers, for example</i> ) |

<sup>25</sup> See Finn *supra* n 14, p. 6.

|   |                                   |
|---|-----------------------------------|
| <b>Telecommunication antennae, satellite connection or WiFi router capabilities</b> | Privacy of personal communication |
| <b>Sprayers used to distribute substances in agriculture</b>                        | None                              |
| <b>Gas detectors</b>  | None                              |

When designing and building a drone, consider what kind of sensors are appropriate for it and what kind of operations it will be used for, depending on the customers you foresee to use the drone. Consider, in addition, what quality of data they should be able to capture and collect. The quality of images captured need not always allow the identification of people recorded. It would not be proportionate to install a very powerful camera with high zoom capabilities on a drone intended as a toy for children, for example. If possible, try to exercise your best judgment when deciding which capabilities would suit the drone, of course, keeping in mind your own legitimate interests as a drone manufacturer and a private entrepreneur.

As manufacturers, your products will have to compete on the market on the basis of the drone features you offer, including the quality of your sensors. Therefore, using lower-quality sensors may not always be your choice. It is important that where drones are equipped with more powerful sensors, they are also equipped with better mitigation measures. These could be software features that enable limiting what data is collected and when or that allow unnecessary data to be automatically erased. Software safeguards will be discussed in greater detail later on in this document.

In addition to the relationship between different sensors and types of privacy affected, it is worth noting that different kinds of information collected is considered to interfere with privacy to different extent. For example, visual recordings of people’s activities and sound recordings of their conversations have a greater impact on their privacy than simple records of the location of a person. Similarly, a continuous video footage has a greater impact than a set of individual images. Finally, recording video footage or images has a greater impact than livestreaming them.

Most drones will likely require some kind of payload and this is especially true for drones used for commercial applications. In addition to choosing the most appropriate payloads, you can enhance the privacy-awareness of drones by empowering drone users to easily control (1) what drone sensors they use, (2) when drone sensors are engaged, and (3) what quality of drone sensors they use / what quality of drone data they collect.

#### Payload and sensor control

During the planning and execution stages of drone operation, drone pilots and operators will have to consider and plan how to minimise their interference with the privacy of individuals and collect as little personal data as possible. As an overarching recommendation, drones equipped with software that allows fine-tuning control over payload sensors can enhance the drone users’ ability to comply with this requirement.

It is recommended that drones are equipped with software capabilities that allow users to control what payload sensors are to be activated and engaged during a flight, effectively tailoring the drone capabilities to what is necessary for their operation. Furthermore, you should incorporate easy user-friendly controls to turn sensors on and off during the flight. Such software could be tailored to allow sensor engagement within a particular flight area or during different parts of a drone flight. In addition, software could allow users to pre-define and document sensors / capabilities use against a pre-planned drone flight. This would support pilots and operators in

easily collecting only the data they need, thus making their activities more respectful to European privacy and data protection regulations. This can assist drone operators and drone pilots in collecting as little personal data about individuals on the ground as possible.

In addition to tailoring sensors used, it would be beneficial for drone users to be able to control the quality of data being collected by such sensors. If you are developing a high-quality commercial drone you may wish to equip it with the highest possible quality of sensors available. These capabilities would be naturally the best choice for a commercial entity, as they would allow a broad range of operation to take place. A few software controls could, however, easily enable drone users to manually choose the quality of data they would like to capture for each individual flight, either before or during the flight itself.

#### Communication capabilities

In addition to other capabilities, drones are equipped with hardware enabling them to communicate with different devices using different channels for a variety of reasons, including to ensure flight safety and enable other drone features. Communication capabilities are most notably necessary for:

- drone controllability through piloting equipment,
- streaming of data captured by drone,
- coordinating drone flight paths with other drones in the same airspace, such as in the context of UAV traffic management systems (UTM),
- ensuring up-to-date databases of geo-fenced spaces,
- communicating electronic identification data by the drone.

Relevant standards will likely be developed at international or European levels to ensure interoperability of drones and different information systems; however, this is still under development. With regard to UTM, there are currently many of projects ongoing testing different ways for drones to communicate.<sup>26</sup> Nevertheless, drone manufacturers are encouraged to closely follow developments regarding communication requirements and follow relevant standards where available to allow for interoperability, as well as ensure the security of data links transmitting information, as will be further detailed below.

#### Drone privacy-enhancing software features

Certain software capabilities can help incorporate privacy considerations into the design and build of drones and increase the control that drone users exert over how far drones interfere with the privacy of those on the ground. This section will examine such software privacy-enhancing features and capabilities.

#### Geo-awareness capabilities

A fundamental way in which drones could be enhanced to respect privacy is by being prevented from entering restricted zones. Member States will be able to define no-fly zones for drones and will have to maintain databases with the location of such zones.<sup>27</sup> A way for these zones to be

---

<sup>26</sup> Eurocontrol, UTM Current State-of-the-Art. <https://www.eurocontrol.int/articles/utm-current-state-art>.

<sup>27</sup> Article 15, *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on rules and procedures for the operation of unmanned aircraft* ([https://eur-lex.europa.eu/eli/reg\\_impl/2019/947/oj](https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj)).



noted is by establishing geo-fences – virtual borders identifying drone-free zones.<sup>28</sup> To respond to this, drone in the C1, C2 and C3 categories will be required to be fitted with geo-awareness capabilities, which would alert pilots or operators when flying in restricted no-fly zones.<sup>29</sup> The requirements for the geo-awareness system, currently proposed, are that it provides:

- An interface to load and update data about airspace limitations in a secure manner,
- A warning alert where a potential breach of airspace limitations is detected, and
- Information on the drone’s status and a warning alert when the positioning or navigation of the drone cannot function properly.

If you equip the drone with geo-fencing capabilities / drone flight control system, ensure the function operates smoothly, without threatening the safety of the drone flight, and it provides information to the drone pilot when geo-awareness capabilities cannot function properly.<sup>30</sup> Moreover, the effectiveness of geo-awareness capabilities depends on drones having access to the latest and most accurate databases of restricted airspaces. It is important to ensure that drones receive timely and secure updates regarding the latest geo-fences and non-flying zones.<sup>31</sup> An interface to load and update such data should be set up that ensures the quality, integrity and validity of the data used.<sup>32</sup> To reinforce this function, consider implementing software controls which would prevent the drone from taking off if its database of geo-fenced or no-fly zones is not up-to-date.

In addition to limiting drone access to nationally restricted no-fly zones, people may wish to keep drones away from their work places or private homes. Similarly, institutions may feel it inappropriate to have drones flying over them, in particular if the buildings are of sensitive nature, such as religious buildings, schools and kindergartens, military facilities, police stations, jails or court houses, hospitals and clinics, etc. – all places which may deserve a special level of protection due to the sensitivity of information which a drone could capture there. Private initiatives have previously existed that allow private persons to designate areas as restricted to drones. In fact, there have been previous attempts to use Wi-Fi positioning to implement virtual drone barriers.<sup>33</sup>

Such initiatives are welcomed and the involvement of drone manufacturers in them is encouraged. Manufacturers may act as an intermediary between such platforms and drone users by enabling interoperability between drones and such initiatives or even launch such a system of their own which allows private persons to designate their own no-fly area. Such initiatives can help support drone operators and pilots in operating drones in greater compliance with privacy and data

---

<sup>28</sup> Gettinger, Dan and Arthur Holland Michel, “Drone Sightings and Close Encounters: An Analysis”, Center for the Study of the Drone, Bard, College, December 2015, p. 17 <http://dronecenter.bard.edu/files/2015/12/12-11-Drone-Sightings-and-Close-Encounters.pdf>

<sup>29</sup> Part 2.13, Part 3.15, Part 4.10, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>30</sup> Part 2.13(c), Part 3.15(c), Part 4.10(c), Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>31</sup> Kruse, Brandao, Jacques and Eva Schulz-Kamm, “Security and Privacy by Design: Securing the Future of UAVs”, 2016, p. 4. [https://rpas-civops.com/wp-content/uploads/2016/11/NXP-Semiconductors\\_DE\\_WP.pdf](https://rpas-civops.com/wp-content/uploads/2016/11/NXP-Semiconductors_DE_WP.pdf).

<sup>32</sup> Part 2.13(a), Part 3.15(a), Part 4.10(a), Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>33</sup> May, Patrick, ‘Virtual Barriers, Manipulation Tools Enlisted to Keep Drones at Bay’, Government Technology, 17 August 2016. <http://www.govtech.com/public-safety/Virtual-Barriers-Manipulation-Tools-Enlisted-to-Keep-Drones-at-Bay.html>

protection requirements and could serve as a mark of quality for drones, fitted with such capabilities.

Such capabilities could be extended to enhance the ability of drones to respect the wishes and, by extension, the privacy of people on the ground. A fundamental part of respecting privacy can be respecting people's wishes not to be filmed. Thus, the database of geo-fenced locations could be extended or supplemented by additional databases, which allow private persons to determine their homes and gardens as no-fly zones for drones.

Finally, geo-awareness capabilities could be extended to geo-fencing capabilities, which do not only alert pilots when a drone enters a restricted space but hinder a drone from entering into that space in the first place, while ensuring the stability and safety of the drone in flight.

#### Direct remote identification

The operation of drones may raise some issues of accountability and transparency, as people may not always be aware of who is operating a drone or for what purpose, nor who to turn to with further questions. A new proposed requirement mentioned in the Commission Delegated Regulation is for drones in classes C1, C2 and C3 to be equipped with a direct remote identification system, intended to counteract this and increase the transparency of drone operations. Such a system should:<sup>34</sup>

- allows the upload of the UAS operator registration number in accordance with Article 14 of Implementing Regulation (EU) 2019/947 and exclusively following the process provided by the registration system;
- ensures, in real time during the whole duration of the flight, the direct periodic broadcast from the UA using an open and documented transmission protocol, of the following data, in a way that they can be received directly by existing mobile devices within the broadcasting range::
  - the UAS operator registration number,
  - the unique physical serial number of the UA compliant with standard ANSI/CTA-2063,
  - the geographical position of the UA and its height above the surface or take-off point;
  - the route course measured clockwise from true north and ground speed of the UA; and
  - the geographical position of the remote pilot or, if not available, the take-off point.
- ensures that the user cannot modify the data mentioned under paragraph (b) points ii, iii, iv and v;

In addition to being a fundamental part of a future UTM system, the electronic identification transmission could help inform people who is responsible for the drone by broadcasting the operator's registration number and, by informing them of the drone's take-off point, could inform them about where they could (potentially) find piloting personnel who could answer their questions and hear out their concerns.

---

<sup>34</sup> Part 2.12, Part 3.14 and Part 4.9, Part 6, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

Remote identification transmissions should take place on the 2.4 or 5 GHz frequency band, using an open and documented transmission protocol.<sup>35</sup> Electronic identification transmissions should be receivable by mobile devices within the range of transmission, allowing authorities and people on the ground access to information about who is operating the drone (the operator) and where they might be able to get more information (the take-off point). This would enhance transparency and accountability of drone operation.

Finally, manufacturers who adopt the direct remote identification transmission could also consider how to protect and enhance the information that can be emitted through such a capability. To protect such information, employ security measures that prevent its unauthorised modification. To enhance it, manufacturers could include a field where operators or pilots could include a message to people around, such as a brief introduction of the drone operation, its general purpose or a reference to a website with more detailed information. As a manufacturer, you are encouraged to think about ways in which drones could enhance the capabilities of operator and pilot to inform people around them of their activities.

#### Logs of flights and activities

To help ensure the accountability of drone users and the transparency of their operations, you can instruct drones to store (at least temporarily) certain operational information such as time-stamps of the latest geo-fencing uploads or of the flight paths uploaded, as well as the paths flown in reality and when payload sensors were engaged. This could serve as evidence of the diligence (or negligence) of drone pilots and operators.

You can also help ensure accountability of drone pilots and operators by implementing a drone interface which logs and tracks the sequence of commands made, as well as actions and changes in the system.<sup>36</sup> For example, where certain drone functions can be personalised and altered, you could keep information about when that was done and, if possible to determine it through access controls, by whom.

#### Automated data minimisation

Once personal data has been collected, consider means through which to minimise it within the system of the drone. This may be possible, for example, if you utilise software that can automatically detect facial features and/or numbers and blur them, following specific instructions. This could support drone pilots and operators in their compliance with data protection legislation in the European Union.<sup>37</sup>

A further safeguard you can apply in this context could be to utilise software which automatically erases all data collected by and stored on the drone after the end of a flight and after the data has been successfully downloaded to another device. Consider how to best develop this feature, e.g. how to allow drone users to deviate from it. Pay special attention to what kind of data may be reasonable to maintain for longer periods of time, perhaps for purposes of accountability and proof of compliance with the law by the drone users. You could allow drone operators and pilots

---

<sup>35</sup> *Ibid.*

<sup>36</sup> See Altawy *supra* n 2, p. 15.

<sup>37</sup> Article 5(1)(c) Regulation 2016/679 (General Data Protection Regulation) specifically requires that only personal data which is “adequate, relevant and limited to what is necessary in relation to the purposes” of the processing is collected and processed.

to determine what data is deleted, what retained and at what point in time through the drone's interface.

Finally, sometimes drones may capture and collect potentially personal data through sensors, intended for the safety of their flight. For example, drone safety can be enhanced by incorporating 'sense and avoid' systems in the drone which allow it to prevent accidents and collisions in real-time by using sensors to detect, track and avoid obstacles around the drone, much like a human pilot would.<sup>38</sup> You could consider how to develop or choose an appropriate 'sense and avoid' system, which would automatically minimise data captured to what is necessary to avoid collisions and accidents – to the outlines of objects and people.<sup>39</sup> This would contribute to the ability of a drone to discard unnecessary data and minimise potential interference with people's privacy.

#### Drone digital security and data protection

Security can play a key role in protecting drones, their controls and the data they store and transmit. Information and IT security is a fundamental pre-requisite for the protection of the data captured by a drone and the privacy of people. A compromised security system could allow drone controls to be overtaken by unauthorised persons and a drone to be used for monitoring of persons without any accountability for those responsible. Moreover, access to data stored on a drone or transmitted by it could impact the privacy of people captured and may result in a data breach, leading to a set of procedural steps for drone users to complete under the GDPR. Therefore, security by design should be attempted alongside privacy by design by ensuring information and IT security for the entire cycle of drone activities.

Some concrete security features would soon become legal requirements. For example, in the Commission Delegated Regulation, drones in classes C1, C2 and C3 should be equipped with safeguards to protect them in case of a loss of data link. It is required that in such cases there are reliable and predictable means to recover the data link or terminate the flight in a way to minimise any impact on third parties in the air or on the ground.<sup>40</sup> Such impact could include privacy impacts. Therefore, manufacturers should consider what safeguards may be appropriate. For example:

- Landing in unplanned locations could be prevented by equipping a drone with a function to automatically return to its take off point in cases of emergencies and errors or to go back and hover at a previous location while re-establishing a data link connection,
- Unauthorised access to data stored locally on the drone, where it lands in unplanned locations, can be prevented through access controls (which could be set temporarily for the particular drone operation) or data encryption.

In addition, the proposed Draft Regulation on drones envisions that untethered drones in the C2 class should be equipped with a data link that is protected from unauthorised access to the

---

<sup>38</sup> See Gettinger, *supra* n 27, p. 18.

<sup>39</sup> Vivet, Laura and Lauren Smith, "Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft", Future of Privacy Forum, 2 August 2016, p. 4. [https://fpf.org/wp-content/uploads/2016/08/Drones\\_and\\_Privacy\\_by\\_Design\\_FPF\\_Intel\\_PrecisionHawk.pdf](https://fpf.org/wp-content/uploads/2016/08/Drones_and_Privacy_by_Design_FPF_Intel_PrecisionHawk.pdf).

<sup>40</sup> Part 2.7, Part 3.7, Part 4.5, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

command and control functions.<sup>41</sup> This requirement is mainly geared at ensuring the safe flight of drones, however, it could also protect privacy by prevent the unaccountable use of drones for data collection by unauthorised persons. This requirement could be further extended to protect a data link from unauthorised access to data and footage transmitted between the drone and command and control equipment, as this could interfere with the privacy of those on the ground.

Security is a fundamental consideration in the build of drones. A holistic approach is required, which considers it as part of every function or equipment on the drone. Drone manufacturers are encouraged to give this due consideration. Of course, you should also keep in mind that there may be legally agreed standards about a particular storage and/or transmission technology that a drone should be equipped with. This may become clearer as advances are made in regulating a UTM system, for example, and should be complied with as they become clearer. Nevertheless, there are other steps that manufacturers can already take now.

For example, using components compliant with security standards or certification schemes could be a step towards ensuring the security of data and communication and could serve as an indicator of the quality of the final drone build and a contributing feature towards its security and safety and, by extension, its ability to protect personal data processed through it. Using certified components could also be noted on the drone as a distinguishing quality feature and as additional information for drone operators and pilots to consider when planning or executing flights. Here, we speak about general information security certification schemes, however, as some drones are connected to the Internet, they may be viewed as Internet of Things (IoT) devices and may benefit from such certification as well.

Offering a more general overview, in the table below you can find an overview of the risks relevant for information and IT security that can arise at different stages of the drone’s functionality and examples of safeguards you can implement to eliminate or mitigate these risks.<sup>42</sup>

|  | Potential risk  | Potential safeguards  |
|--|---|---|
| <b>Overall information and IT security assurance</b> | Malicious hardware or software could be used to attack both the drone and the ground control systems. <sup>43</sup> Such vulnerabilities could lead to loss of sensitive data or to loss of control over drones while operational, both of which could raise potential privacy and security concerns. | <p>The security of the entire supply chain of software and components you use to manufacture a drone should be ensured.</p> <p>Ensure that the update or patching of software does not interfere with the operation of the drone, especially while in flight.</p> <p>Using firewalls, antivirus systems and intrusion detection systems could be a fundamental step towards security the drone.</p> |

<sup>41</sup> Part 3.8, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>42</sup> See Altawy *supra* n 2.

<sup>43</sup> An example of drone-specific malware is Maldrone, which allows an attacker to take over control over a drone and to inject information in flight control communications to the drone and sensor readings sent by the drone.

|  |  |  |
|--|--|--|
| <b>Drone navigation, both when operating autonomously and manually</b> | Information and IT security vulnerabilities in the ground control system for the drone or in the transmission of information and commands between the drone and its controlling point could allow unauthorised persons to take over control of the drone or disrupt its normal functioning. This could raise concerns about the privacy of people on the ground since this unauthorised controller would be unknown to them but could also raise security issues due to the physical damage and harm which drones could cause. | Installing authorisation controls on the ground control system could help limit unauthorised access and control of the drone or unauthorised interference with drone features and settings.  |
|  | Since Global Navigation Satellite Systems (GNSS) like Galileo, GPS or GLONASS broadcasts are freely accessible, unencrypted and unauthorised signals, a drone could be fed misleading GNSS signals to alter its calculations of geographical coordinates. <sup>44</sup> This could lead to a drone changing its flight path and could raise privacy and security concerns, particularly when the drone is operating autonomously.  | Software features which are able to detect fake GNSS signals should be incorporated into the product.<br><br>A interface feature whereby manual control can easily be restored and override autonomous operation is recommended.   |
|  | GNSS signals could also be jammed. This would disrupt the connection between the drone and external navigation, leading to the drone becoming disoriented and potentially crashing. <sup>45</sup>  | Alternative means of navigation could be considered, such as reliance on visual and inertia cues and requiring the attention of pilots and operators to begin manual operation. The use of GNSS receivers for more than one system can also mitigate the risk of GNSS jamming. |
| <b>Data collection and processing</b>                                  | The operation and functioning of drones could be attacked by injecting false sensor data into the flight controller. This type of attack can impact all types of drone sensors, including radar, infrared and electro-optical sensors.   | A drone could utilise alternative operational procedures to compare data received through different sensors and crosscheck readings. This could allow the drone to tolerate malfunctioning components or infected information.   |
| <b>Data transmission between the drone and other devices</b>           | Real time data streams can be hacked and intercepted, especially if they are not encrypted or equally protected. This can jeopardise the privacy of people captured in the data, as well as  | Incorporating continuous mutual authentication between the operator and the drone can help authenticate communication.   |

<sup>44</sup> See Altawy *supra* n 2, p. 9

<sup>45</sup> *Ibid.*

|                              |   |  |
|------------------------------|---|--|
| <b>(e.g. control system)</b> | the security of the drone operation itself by failing to control access to key data.  | Encryption could help protect such data.<br><br>Utilising security keys to authenticate the connection and transmissions can ensure its security.  |
| <b>Data stored on drone</b>  | By exploiting information and IT security vulnerabilities, unauthorised personnel could gain access to data stored on a drone. This could take place in the event of a drone accident or drone crash, as well as by exploiting vulnerabilities in the hardware and software of the drone. This could raise privacy concerns for individuals whose data is captured. | Use encryption to ensure the data stored on a drone is protected.<br><br>Implement access controls to the drone itself requiring authorisation for accessing data.<br><br>Build in capabilities to detect data breaches and alarm users to them. |

## Drone packaging and privacy

Provide drone pilots and operators with information

As part of your role as a drone manufacturer, you will be required to provide certain information to your consumers, including, depending on the class of your drone, how to operate it, its specific characteristics, limitations and controls, as well as the risks of operating drones. There is broad agreement among experts that raising awareness among drone users about airspace rules and guidelines for responsible drone operation is a key step to achieve safe and secure flights.<sup>46</sup> Moreover, informing drone users of the precise capabilities and features of the drone and how to use them can allow them to implement them in ways that support their operation in line with data minimisation requirements and respect for privacy.

At a fundamental level, all drone classes are required to come together with sufficient instructions in the drone packaging or otherwise to allow remote pilots to safely control the drone.<sup>47</sup> In addition, further information has to be included for some classes of drones as well. C0 drones (less than 250 g MTOM) and C4 drones (model aircrafts) should come with some information materials, including a set of clear operational instructions, the technical characteristics of the drone and its limitations, and highlighting risks related to drone operations.<sup>48</sup> Larger drones for general use – C1, C2, C3 drones should also come with a user manual that adds more details of information, including the functionality of the geo-awareness features, maintenance and

<sup>46</sup> See Gettinger, *supra* n 27, p. 19.

<sup>47</sup> Part 1.4, Part 2.4, Part 3.3, Part 4.3, *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>48</sup> Part 1.8, Part 5.4, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

troubleshooting instructions.<sup>49</sup> The risks highlighted in such documents should be tailored to the particular drones and the users envisioned for those drones. These risks may include privacy risks.

By providing detailed guidance to users about how to fly the drone, pay attention to introducing users to all features, especially those relevant for privacy – sensor controls and engagement, data security and encryption, relevant access controls. Moreover, to ensure clarity, all information provided to drone users should be offered in language that is accessible and appropriate, considering the likely users of the drone.

Finally, manufacturers will also be required to include an EASA-approved information notice in the packaging of their drone. This notice will introduce drone users to applicable limitations and obligations of the drone operation.<sup>50</sup> Related to this, a set of proposed consumer information posters could already be found on the website of EASA, though they are not final.<sup>51</sup>

In addition, where you believe that additional information to the EASA-approved leaflet may be relevant or appropriate, we recommend that you consider providing additional information leaflets with key privacy, security and insurance risks and recommendations as to how to operate drones in a responsible manner. For best measure, it would be beneficial if you include a link to the DroneRules PRO website as well. In Annex to this document you can find leaflets you can readily use. These leaflets are intended to complement and not replace EASA-approved leaflets.

#### Labelling of drone

Equally, drone operators and pilots should be aware of the details of the specific drone they are operating in order to best plan their drone operations and easily check the drone capabilities. Clearly marking a drone to that effect could help them in this regard. Where a drone complies with the relevant technical and safety requirements laid down in the proposed Draft Regulation for a particular class, it should be clearly labelled to that effect. This is a requirement for all drone classes, intended for use in ‘open’ category operations, and includes a label of the Class type (i.e. C0, C1, C2, C3 or C4), as well as a CE certification marking.<sup>52</sup>

In addition, a unique serial number, compliant with standard ANSI/CTA-2063 should be provided and affixed to the drone and the user manual (or drone packaging) in a legible manner for C1, C2 and C3 drones.<sup>53</sup> This information can help operators register their UAs, where necessary, and will form part of the information transmitted by the drone’s electronic identification system, enhancing the transparency and accountability of drone flights.

---

<sup>49</sup> Part 2.18, Part 3.19, Part 4.15, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>50</sup> Part 1.9, Part 2.19, Part 3.20, Part 4.16, Part 5.5, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).

<sup>51</sup> EASA, “Flying a Drone – do’s and don’ts”, Proposed Consumer Information, 2018. [https://www.easa.europa.eu/sites/default/files/dfu/217307\\_EASA\\_DRONE\\_POSTER\\_2018%20final.pdf](https://www.easa.europa.eu/sites/default/files/dfu/217307_EASA_DRONE_POSTER_2018%20final.pdf)

<sup>52</sup> Article 16, *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>). Part 1, Part 2, Part 3, Part 4, Part 5 in Annex.

<sup>53</sup> Part 2.11, Part 3.13, Part 4.8, Annex to *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems* (<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN>).



Finally, as was mentioned above, you could also take steps and note the use of components that are compliant with security standardisation or certification schemes on the drone to distinguish drone's quality for potential users and provide an easy way to check and reference relevant security features of the drone.

## How to apply these principles in practice

Applying the above principles and features in practice may seem overwhelming and confusing at first. For this reason, we suggest a step-by-step approach utilising a Privacy Impact Assessment (PIA) methodology – understanding intended or foreseeable operations, identifying risks and then considering appropriate safeguards and how to implement them (please note that a PIA is not a comprehensive Data Protection Impact Assessment as set out in Article 35 of the GDPR). You can use the following questions to help structure your planning activities. Tailor these questions to the specific drone you are manufacturing and consider how it may be used. Ask further questions that you consider relevant to your activities.

|                      | <b>Fundamentals of your drone</b>   | <b>Data collection</b>  | <b>Data storage</b>  | <b>Data processing</b>   | <b>Data erasure</b>  |
|----------------------|---|---|--|--|--|
| <b>Data mapping</b>  | <p><b>Understand the background of your drone</b></p> <p>What is your drone? What is it designed for? What are the likely scenarios in which it will operate?</p> <p>What category / class is it in?</p> <p>How does your drone navigate?</p> <p>Does your drone have extra features, such as autonomous flight, follow-me functions?</p> | <p><b>How does your drone capture (collect) data?</b></p> <p>What sensors does it have? What type of sensors are they? How powerful are they?</p> <p>How can they be controlled, when are they actively engaged?</p> <p>What type of data does the drone collect? Include here all types of information on which the drone relies, including GNSS coordinates, WiFi signals, etc.</p> | <p><b>How does your drone store data?</b></p> <p>Is data recorded? Is it recorded on the drone or transmitted?</p> <p>If data is transmitted, how is it transmitted? What communication channels are used and what is the recipient device?</p> <p>If data is stored on the drone, what storage media is used?</p> | <p><b>How does the drone process data?</b></p> <p>Does data undergo any additional processing inside the drone? For example, is the drone equipped with software capabilities to carry out automatic blurring of faces?</p> <p>Is the data processing automatic?</p> | <p><b>How does the drone erase data?</b></p> <p>How long is data held by the on the drone/ equipment? At what point in time is it erased?</p> <p>Is erasure automatically scheduled? Can this be manually overwritten?</p> |
| <b>Risk identifi</b> | <p><b>Are there any risks regarding your drone in general?</b></p>  | <p><b>What privacy and data protection risks arise from the drone capturing data?</b></p>   | <p><b>What privacy and data protection risks arise from the drone storing data?</b></p>  | <p><b>What privacy and data protection risks arise from the drone processing data?</b></p>   | <p><b>What privacy and data protection risks arise from the drone erasing data?</b></p>  |

|                                     | Fundamentals of your drone  | Data collection   | Data storage   | Data processing  | Data erasure   |
|-------------------------------------|---|---|--|--|--|
|                                     | <p>Are you complying with all legal requirements related to your drone class (as regulated by EASA), including privacy, safety and security requirements?</p> <p>Are there any risks or vulnerabilities in the navigation of your drone?</p> <p>Is the drone sufficiently agile to easily navigate as necessary for its likely uses?</p> <p>Are there any risks or vulnerabilities in the autonomous and semi-autonomous functions of your drone?</p> | <p>Is personal data (likely) to be captured? Is one of the seven types of privacy impacted (bodily privacy, privacy of data and image, privacy of location and space, of behaviour and action, of association, of personal communication, or of thoughts and feelings)?</p> <p>Can the data capturing be minimised, e.g. could users easily operate the sensors by turning them on and off when they wish, could they specify what quality of data they wish the sensors to capture?</p> <p>Is data verified and sensor accuracy ensured during collection?</p> | <p>Is the data stored on the drone protected from access by unauthorised people?</p> <p>Is data stored on the drone encrypted?</p> <p>Is data transmitted by and to the drone protected from unauthorised capture or interference?</p>   | <p>Can the data processing features be easily turned on and off by users?</p> <p>Can the data processing features be easily personalised by users?</p>   | <p>Is the period of automatic deletion of data stored on the drone appropriate?</p> <p>Can users easily personalise data erasure features on the drone?</p> <p>Is erasure secure and irreversible?</p>   |
| <b>Safeguard identification and</b> | <p><b>How can you eliminate or mitigate risks related to the drone in general?</b></p> <p>What steps do you need to take to ensure you comply with your legal requirements as a manufacturer for this particular drone class?</p>   | <p><b>How can you eliminate or mitigate risks related to data collection by the drone?</b></p> <p>Can you use drone hardware or software which allows drone operators and pilots to easily customize the drone's capabilities, e.g. by implementing modular design</p>  | <p><b>How can you eliminate or mitigate risks related to data storage by the drone?</b></p> <p>What kind of information and IT security measures can you employ to limit access to data stored on the drone and data transmitted by and to the drone from control devices?</p> | <p><b>How can you eliminate or mitigate risks related to data processing by the drone?</b></p> <p>Can you place easy-to-use controls on the drone software for each individual software feature?</p> | <p><b>How can you eliminate or mitigate risks related to data erasure?</b></p> <p>Can you implement automatic procedures for erasure of data from the drone after it has completed its operation and relevant data has been downloaded? Can this</p> |

| Fundamentals of your drone  | Data collection  | Data storage   | Data processing   | Data erasure  |
|---|--|--|---|---|
| <p>What safeguards could you implement to ensure the safe and reliable navigation of your drone?</p> <p>Could you include additional navigational features, including providing different cruising speeds or ease of navigation?</p> <p>What safeguards could you implement to ensure the secure and reliable functioning of your drone's autonomous and semi-autonomous features? Could human pilots easily and quickly override such functions?</p> | <p>allowing easy changes in drone payloads, by using interfaces which allow users to control the quality of data captured by sensors or which allow users to easily turn sensors on and off?</p> <p>Can you equip your drone with some privacy-preserving features, such as automatic anonymisation of visual recordings?</p> <p>Could you implement safeguards to ensure the accuracy of captured data? Would it be possible to cross-check data captured by different sensors? Would that be necessary or appropriate, considering the drone's likely use?</p> | <p>Such safeguards could include access controls, encryption, continuous verification of the identity of sending and receiving devices, etc.</p> | <p>Can you implement data processing features which would minimise any personal data captured, by removing or blurring e.g. numbers of houses or car plates, faces?</p> | <p>procedure (and when it occurs) be easy to operate and personalise for drone users?</p> <p>Are there any steps you can take to ensure that data erasure from the drone is irreversible?</p> |

## Conclusion

As drones are used in diverse fields, their impact on privacy and data protection is clearer and better studied. Drone operators and pilots face a multitude of regulations and requirements that they need to comply with when planning or carrying out drone flights, including these requirements. Drone manufacturers and producers can play a key role in supporting operators and pilots to comply with these requirements and may, themselves, soon be under legal obligations to equip some drones with features that enhance privacy. In addition, drones that allow and support responsible drone use lie at the basis of drone acceptance and legal compliance in Europe.

This guide has been intended to help manufacturers understand what concrete steps they can take to enhance their drones during design, development and production stages, as well as to introduce them to some of the requirements in the Commission Delegated Regulation. Nevertheless, manufacturers are encouraged to consider how to extend or enhance such features and equip all drones they produce with suitable and proportionate privacy-enhancing features with the help of this Guide.

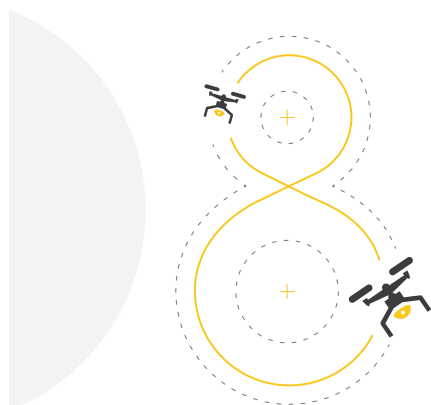
# Annex I Data Protection and Privacy Leaflet

DroneRules<sup>eu</sup> PRO

Annex I Data Protection and Privacy Leaflet

## Operating your drone in a responsible manner: privacy and data protection

If you operate your drone in the vicinity of people, you may be exposed to privacy and data protection risks. Privacy and the protection of personal data are both recognised as fundamental rights in the European Union and are legally enforceable. With the General Data Protection Regulation (GDPR), you are obliged to take certain steps to ensure you treat the personal data you capture with your drone in a responsible and secure manner. You should be informed about the risks and safeguards you are required to take by law and out of respect for others.



DroneRules.eu has identified 8 guiding principles for professional operators to keep in mind to support compliance with the GDPR when they collect personal information.

### 1 Inform

Whenever you capture or record any information about a person, especially clear images of their face, inform them about it. Draft a public privacy statement to provide further transparency.

### 2 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.

### 3 Minimise

Always think about what kind of drone to use and how so that you capture the least amount of data about people in the area of your operation. Anonymise data where possible. Blurring faces, house and car numbers may help you alleviate your GDPR obligations.

### 4 Respect

Ensure that people can exercise their rights to object to data collection processing, change their mind about it or have their data removed. Remember, people also have the right to access their data, receive a copy of their data and correct it.

### 5 Limit

The purpose for which you use the data to the purpose you originally stated and limit the storage of the personal data to the minimum period required.

### 6 Protect

Provide adequate security for the personal data and do not share it with third parties without informing individuals and ensuring data will be protected with its recipients. Share only anonymised data if possible.

### 7 Assess

Act responsibly and plan your activities with privacy in mind (privacy-by-design). If your activities pose a high risk to the rights of people on the ground, conduct a data protection impact assessment (DPIA). See DroneRules.eu resources for guidance and templates.

### 8 Demonstrate

Document your flight and the steps you have taken to make it proportionate and privacy-aware. Ensure that you can demonstrate that you have a lawful basis for your activities, e.g. consent from data subjects.

Following these principles will considerably reduce your risks when collecting and processing personal information via a drone.

Find more information, including handbooks, templates and other resources on the [DroneRules.eu](https://www.droneules.eu) website.



# Annex II Security and Safety Leaflet

DroneRules<sup>eu</sup> PRO

Annex II Security and Safety Leaflet

## Drone Safety and Security during Flight

As a drone operator and a drone pilot, it is your responsibility to ensure that drones are operated in a safe manner as far as possible. Although not a complete list, here are a few tips for operating in a safe and secure manner.



### SAFETY

be informed and prepared

- **Check the legal requirements of your operation.**

New Regulations will guide how drones should be operated for 'open' and 'specific' categories flights. Make sure to check what legal requirements and limitations apply to your flight and comply with them.
- **Check your location**

Inform yourself about the location and surrounding areas where you plan to fly a drone. In particular, make note of any designated no-fly or restricted zones and ensure you have the latest information about any geo-fenced locations. Plan your flight in a way to comply with such limitations.

Enable geo-awareness or geo-fencing capabilities whenever your drone is equipped with them. Make sure to regularly update your database of geo-fenced locations and, at best, try to do so before each drone operation.
- **Check the weather**

As a last step before the flight, make sure to check the weather on the ground. Be careful to only use drones in an environment that they are designed to withstand.

### SECURITY

protect drones and data

- **Protect drones and data during transmissions**

Protect drones from being hijacked and from unauthorised persons gaining control over them. Moreover, protect data transmitted by a drone and communicated to other equipment from being intercepted, corrupted or viewed by others.

You can do this, for example, by:

  - placing access controls on command and control functions
  - securing the data link between the drone and piloting equipment, for example through encryption.
- **Protect data on drones**

Protect data stored locally on drones from being accessed by unauthorised persons by ensuring security measures are enabled and in place, for example:

  - regularly delete older data from drones,
  - place access controls to view data stored on drones,
  - encrypt data stored on drones.

More information about drone safety and security and guidelines for responsible drone use can be found on the website [DroneRules.eu](https://DroneRules.eu)

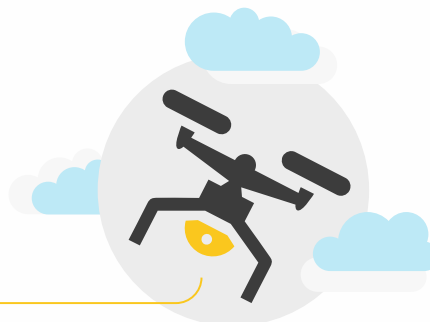
# Annex III Insurance Leaflet

DroneRules<sup>eu</sup> PRO

Annex III Insurance Leaflet

## Protect yourself and be insured

When using drones for professional commercial reasons as an operator, you are obliged to purchase Professional Liability insurance to protect your assets and cover any damage your equipment or your employees or contractors cause during their operation of a drone. The following steps can help you ensure you choose the right insurance for yourself.<sup>54</sup>



### Step 6

#### Maintain information up-to-date

Remain in contact with your insurer and inform them if you start carrying out new activities, if the activities you have declared significantly evolve or if you are not sure whether such activities are already covered by the insurance policy.

Ensure that your insurance policy and insurance certificate clarify that you are covered for your specific activities.

### Step 4

#### Make sure the limit of liability proposed by the insurance is sufficient

Consult with Regulation (EC) 785/2004, a regulation ensuring that victims of accidents have access to adequate compensation, to identify the minimum level of insurance coverage per accident required, depending on the Maximum Take-Off Mass (MTOM) of the drone. Identify the appropriate level of insurance for you.

### Step 2

#### Check the scope of cover of your contract

Make sure that your Professional Liability insurance covers liability for accidental bodily injuries, as well as accidental damages to property that result from drone operation. Also take note of any territorial limits to your insurance coverage.

### Step 5

#### Get an Insurance Certificate

To be sure that you are insured, ask your insurance company for an insurance certificate that clearly states you are protected when operating drones for commercial purposes.

### Step 3

#### Check the exclusions listed in your contract

Carefully look at what exclusions there are in your insurance, i.e. in what cases the insurer does not have to pay you. Such exclusions will inform you what kind of risks are not covered by your policy.

### Step 1

#### Declare all your activities in the policy schedule

Make sure that the activities you undertake with drones are properly declared to the insurance company. You can do this by mentioning it as part of your business in the policy schedule.

Ensure that drone operations are either specifically listed or otherwise covered in your insurance contract.

More information about drone safety and security and guidelines for responsible drone use can be found on the website [DroneRules.eu](http://DroneRules.eu)

<sup>54</sup> DroneRules.eu, Insurance Checklist. <http://dronerules.eu/en/professional/resources/pdf/1349>.