# DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

A DroneRuels.eu PRO resource for drone operators and pilots

DroneRules PRO

# Data Protection Impact Assessment Template

## Table of Contents

# About this handbook & template

## What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) is a risk management procedure that is required in Article 35 of the General Data Protection Regulation (GDPR) whenever personal data is processed and when such processing is "likely to result in a high risk to the rights and freedoms of natural persons".

To counterbalance processing that may present high risks to data subjects (people whose personal data is processed), a DPIA is a tool that allows you to critically examine a data processing activity and to assess it against data protection principles and legal requirements.[1] In doing this, the DPIA will help you identify risks and assess their impacts and, based on the identified risks, the DPIA will guide you to plan for appropriate solutions and safeguards to eliminate, mitigate or transfer relevant risks.
Thus, a DPIA requires the following:[2]

(1) mapping of drone flight / data flows – a systematic description of the processing,[3]
(2) identification of the necessity and proportionality of the processing – necessity and proportionality of the risks are assessed,[4]
(3) risk identification and assessment of impact – the risks to individuals whose data is processed are identified,[5]
(4) solution identification and assessment of impact –risks to individuals whose data is processed are mitigated and managed.[6]

You can complete a DPIA for each of your operations or you can use the same assessment for a set of similar operations. Operations, which cover the same activities in similar contexts do in general not require more than one DPIA. Similar operations also include operations jointly conducted by several entities. Thus, the same DPIA may be used by two controllers working closely together in an operation. However, you cannot use the same assessment for all your activities when they differ significantly.

The DPIA is designed to guide you through some of the key aspects which can have an impact on your interference with personal data. The template will make you consider how proportionate and necessary your personal data processing is, considering:

- your lawful basis and the purpose of your operation,
- your data minimisation, including when collecting, retaining and sharing personal data with other data recipients, processors and especially when transferring data outside the EU or EEA.

Moreover, the DPIA template will ask you about how you protect the rights of data subjects (the people whose personal data is processed). Such questions will relate to:

- the proportionality and transparency of your activities and how informed data subjects are,

[1] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248, 4 April 2017, p. 4. (Called Article 29 Working Party, Guidelines on DPIA below). http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
[2] Article 29 Working Party, Guidelines on DPIA, p. 21.
[3] Article 35(7)(a) GDPR
[4] Article 35(7)(b) GDPR
[5] Article 35(7)(c) GDPR
[6] Article 35(7)(d) GDPR

- the exercise by individuals of their rights, in particular the right to access and portability, the right to rectify, erase, object or restrict processing.

## Why should you use this template?

### Benefits throughout the entire cycle of the drone operation(s)

This template provides you with a structured approach and a set of guiding questions to help you identify key pieces of information about your drone operation, which will prompt you to plan and carry out a privacy-aware drone mission by making you consider the privacy risks presented by your drone operation and identify appropriate safeguards to tackle them. This DPIA template can provide you with the following benefits throughout different stages of your operation.

| | |
|---|---|
| **Planning stage** | • Use this template to incorporate privacy and data protection considerations into the design of your activities. This will assist your compliance with the principles of privacy by design and data protection by design and default and will support your acting in an ethical and privacy-aware manner.<br>• Use this template to develop an optimal plan for your drone mission which would minimise your exposure to legal risks, while optimising your use of drones. |
| **Execution stage and the drone flight(s)** | • Provide a copy of the completed DPIA template or its summary to your employees to ensure the drone operation is carried out in compliance with your plans. Specifically, provide the piloting team with key information about the flight path, flight equipment and other safeguards which they should implement during the flight itself. It is important that you implement the safeguards identified in your own risk assessments when operating the drone. |
| **After the flight(s)** | • Once completed, use this template to audit yourself, the mission execution, and your employees against your plan.<br>• Use this template and the safeguards you have committed to, as a basis for the data-handling policies and procedures you implement internally.<br>• Use the DPIA template, along with other documents, as proof of your compliance with privacy and data protection principles if audited by external parties and competent authorities. |

### A template tailored to your needs

Finally, this DPIA template is specifically designed to guide you in understanding and applying GDPR requirements to drone operations. The content and questions of this DPIA template have been tailored to drone professionals – operators and pilots, providing you with a targeted resource that is intended to identify risks that might be more commonly raised by drone use. However, this template does not provide you with automated advice. It is up to you to use this template together with the GDPR and the other DroneRules PRO resources and complete it using your best judgment. As you progress through this template, the perspective of individuals on the ground should guide your responses.

## How should you use this template?

This DPIA template will help guide you through the different steps of a DPIA by asking you questions about your flight(s), the data protection risks that your operations could give rise to. Drone operations could interact with data protection requirements in a few different ways and this template will ask you to describe and systematically examine your:

- drone flight – location, flight path, duration and context
- the equipment you use, and
- the data management practices for collected data and guiding you to identify where your operations give rise to data protection risks.

You should complete a DPIA before you begin your flight.[7] This will provide you with sufficient time to complete it and implement in practice any safeguards you have identified. However, a DPIA is not a one-time exercise and you should adapt it to any changes you make to your drone operation to accurately reflect it. This will ensure it remains relevant.

Save a copy of any DPIAs performed with this template. You can save this to your archives and use it as documentary proof to supplement your compliance with the GDPR.

You may consider publishing that you have undertaken a DPIA or sharing parts of your DPIA or a summary of the results to publicly demonstrate your privacy-aware behaviour and gain people's trust and confidence in your activities.[8] However, you should refrain from making publicly accessible information that could give rise to risks for your operation or your business, such as:

- detailed information on security measures and precise hardware and software used that could reveal cybersecurity vulnerabilities;
- information about your operations, partners, clients, which could reveal trade secrets or sensitive commercial data relating to your business operations.

Use this template together with other DroneRules.eu resources.

## Who should be involved in a DPIA?

*Working with a DPO*
When carrying out a DPIA, it is recommended that you involve experts and interested parties. To ensure you carry out a DPIA in a correct manner, you should seek the guidance and advice of your Data Protection Officer (DPO), if you have appointed one.[9] A DPO will also be responsible for monitoring the implementation of the DPIA in practice.[10]

*Collaborating with data processors*
If your operation includes the use of a data processor, collaborate with them to receive all necessary information to complete this template. The same applies with regard to any clients or joint controllers where they hold information necessary for this DPIA template. This is especially true for information regarding sharing data with third parties within the EEA or in third countries.

*Consulting with stakeholders*
Moreover, where it is practicable, you are also encouraged to consult with data subjects or their representatives, when completing a DPIA.[11] For drone missions carried out in populated areas, this could be done by, for example, consulting with local business and residents, neighbourhood panels, institutional, educational, medical, political or religious establishments close-by.[12] This would both help you assess the impact of your activities, as well as inform local communities of your operations. Where this is not appropriate or impossible, you can document the reason you did not pursue external consultation. Where you have carried out a

[7] Article 35(1) GDPR
[8] Article 29 Working Party, Guidelines on DPIA, p. 17.
[9] Article 35(2) GDPR
[10] Article 29 Working Party, Guidelines on DPIA, p. 13.
[11] Article 35(9) GDPR
[12] Stakeholder consultations could also include consultations with your colleagues from different departments within your organization which could provide diverse considerations.

consultation but decide to act contrary to some of the stakeholder input, document your reasons for doing so.

*Working with authorities for higher risk processing*
If, upon completing this DPIA template, you conclude that your activities continue to pose a high risk to the rights and freedoms of people affected by your drone operation, despite the safeguards you have considered and you can implement, you should contact and consult with your national or local supervisory authority before carrying out your mission.[13] This could be the case where you have identified a serious risk which you are unable to mitigate.

In such cases you should turn to your relevant data protection authority with all relevant information as described in Article 36 GDPR. The data protection authority will then, after a period of eight weeks (which may be extened by another six weeks), provide you with advice how to carry out the data processing. This is a legal requirement and a procedure that should be followed whenever required.

[13] Article 36 GDPR

# Step 1: Do you need a DPIA?

## When are you legally obliged to carry out a DPIA?

There is an obligation to carry out a DPIA when a personal data processing is likely to result in a high risk to the rights and freedoms of people. This obligation falls on data controllers – natural or legal persons who determine the purposes and means to collect and use personal data.[14]

Moreover, this obligation only applies where personal data is processed. Personal data is data which allows the identification of individuals. Blurry images or glimpses of people from a great distance would likely not be considered personal data, however images of people's faces or recognisable clothes, haircuts, as well as the license plates of their vehicles could be considered personal data. Moreover, even blurry images can, together with additional information, qualify as personal data (e.g. if the name of a person subject to drone surveillance is known, blurry images may allow tracking his or her movements). Also, personal data can take many shapes and forms, including videos or still images.

Processing personal data is considered to pose a high risk to individuals in particular if one of the following is true:

(1) You carry out systematic and extensive evaluations of people (based on automated processing) leading to real-life consequences for them, e.g. ability to take out a loan or acceptance in an educational institution.[15] This could be the case if the personal data you collect is used to determine whether individuals or a neighbourhood receive certain benefits, e.g. construction or infrastructure projects.

(2) You capture significant amounts of potentially sensitive data, such as information about people's political opinions, religious beliefs or criminal records.[16] This could be the case if you capture on a regular basis individuals going in or out of religious buildings, medical facilities, police stations, political party headquarters or sexually-relevant areas, e.g. red light districts. One-time events or operations where only a limited amount of individuals are concerned, will most likely not qualify as "significant amounts"). This would make it possible to make assumptions of their opinions, beliefs or personal preferences.

(3) You carry out systematic monitoring of public spaces on a large scale,[17] e.g. large-scale CCTV. This could be the case where you fly repetitively or for a prolonged period of time over the same area.

If one of the above conditions is true and you (or your company) is a data controller for this personal data processing, *you are legally required* to carry out a DPIA before you proceed with any personal data processing. It is recommended that you consult with data protection experts and/or your national data protection authority.

[14] Article 4(7), GDPR.
[15] Article 35(3)(a) GDPR
[16] Article 35(3)(b) GDPR
[17] Article 35(3)(c) GDPR

## When are you likely to be legally obliged to carry out a DPIA?

There may be more situations where personal data processing activities are also likely to pose a high risk to the rights and freedoms and individuals. National Data Protection Authorities (DPAs) offer further guidance about when they consider personal data processing to pose high risks. This will help you determine whether your activities require a DPIA. You can find concrete documents that clarify the approaches of all EU DPAs online here. However, some guidance about when a DPIA may be required can also be found below:

(1) The processing itself prevents individuals from being able to exercise a right or to use a service or a contract.[18] This could be the case where processing takes place in the public area where individuals are unable to avoid it, prevent or escape it.

(2) Data is collected and processed on a large scale. Large scale could refer to the number of people concerned, the volume and range of data processed, the duration of data processing or the geographical extent of the processing;[19]

(3) You use innovative. experimental and/or powerful new technology.[20] New forms of data collection and usage require consideration about what kind of risks they pose to the rights and freedoms of individuals. This could refer to, for example, Internet of Things equipment, facial recognition or high resolution, high speed cameras.

(4) You consider sharing data with another organisation, especially if such an organisation is located outside the borders of the EU or the EEA;[21]

(5) You plan on capturing information about vulnerable individuals – people who may be unable to oppose being captured or to fully understand the consequences of being captured. This could include employees, children, the elderly, medical patients, asylum seekers or mentally ill;[22]

(6) The data collected could be repurposed, matched or combined with other data. In this way, data from multiple sources could potentially be processed for different purposes than originally intended, purposes which would exceed the reasonable expectations of individuals.[23]

If one of the above conditions is true and you (or your company) is a data controller for this personal data processing, *you may be legally required* to carry out a DPIA before you proceed with any personal data processing. It is recommended that you consult with data protection experts and/or your national data protection authority for their concrete guidance. You can find country-specific information about when a DPIA is required here.

[18] Article 22, recital 91 GDPR; Article 29 Working Party, Guidelines on DPIA, p. 9.
[19] Article 29 Working Party, Guidelines on DPIA, p. 9.
[20] Recitals 89 and 91 GDPR, Article 29 Working Party, Guidelines on DPIA, p. 9.
[21] Article 29 Working Party, Guidelines on DPIA, p. 9.
[22] Recital 75 GDPR, Article 29 Working Party, Guidelines on DPIA, p. 9.
[23] Article 29 Working Party, Guidelines on DPIA, p. 9.

If you are under a legal obligation to carry out a DPIA and you fail to do so or you do so in an inaccurate manner, you may face administrative fines. The GDPR sets the maximum fine as up to 10M€ or up to 2% of the total worldwide annual turnover of the undertaking of the preceding financial year, whichever is higher.

### When are you NOT legally obliged to carry out a DPIA?

There are situations in which you are not legally required to carry out a DPIA. This would be where:

(1) You are not a data controller – this would be where you are a drone operator and you have contractually shifted this role on to someone else,

(2) your drone operation falls within an exception to carry out a DPIA, that has been determined by your relevant data protection authority,[24]

(3) you are acting to comply with other or competing legal obligations or to carry out a task in the public interest, provided there has been an impact assessment during the legislative process and unless your relevant national law states that you need to carry out a DPIA regardless.[25] This means that if the law requires you to act in a certain way, this would not compromise your compliance with the law and would not require that you carry out a DPIA.

In addition to the above, it should be repeated that there is no requirement in general to carry out a DPIA and a DPIA will only be necessary in a set of high-risk circumstances. Where your drone operation does not include personal data processing that falls within any of the above cases nor within cases identified by your relevant national authorities as high-risk processing activities, you will not need to carry out a DPIA.

[24] Article 35(5) GDPR
25 Article 35(10) GDPR

## Step 2: Map your operation and your personal data flows – what is the personal data processing?

The questions in this section will help you create a map of your operation, its context and the personal data flows within your business in clear terms. This will support you in assessing the nature, scope, context and purpose of your activities and to identify the sources of any privacy and data protection risks they raise. Specifically, the DPIA template will help you lay out:

- how your drone operation will take place; and
- how data, namely personal data,[26] will be collected, recorded, processed and anonymised or deleted.

Using this map, you will then be able to identify relevant privacy and data protection risks which could arise during or as a result of your operation, as well as decide on appropriate safeguards to mitigate such impacts.

*** Refer to the other DroneRules PRO resources when completing this section. ***

| Data mapping | Guidance |
|---|---|
| **What operation is being undertaken? Please describe the purpose of the flight, the location and its duration, if known.** | *Describe in a few words your drone operation(s). If your drone operation has a name or an identification number, you can add it here as well.*<br><br>*Describe:*<br>- *the reason for the operation. If you are operating within the framework of a specific event or project, add that.*<br>- *the location and area of your planned drone mission(s). Consider and mention whether there are people around, whether it is a commercial or residential area, whether there are special buildings around, e.g. school, church, jail, whether you will operate near a private or semi-private space, e.g. a secluded lake or beach.*<br>- *the time of the flight, the duration and the time of day.* |
| | |

[26] Personal data refers to any information which can allow the identification of individuals, whether by you or by third parties. This includes images of their face, recognisable clothes, hairstyles, their car and its plate number, their houses and homes along with their location.

| | |
|---|---|
| **What kind of personal data will be collected? Describe the type of personal data that may be collected and what kind of data subjects would likely be affected.** | *Consider what kind of payload, sensors and software your drone will be equipped with and what the purpose of your mission(s) is. Try to describe whether you are looking to capture visual data, such as images or video, or audio, such as sounds, conversations. Only describe the personal data you will collect.*<br><br>*Consider whether any of the data you could collect would be of a sensitive nature to individuals on the ground, e.g. bodily images, biometric data, information about sexual orientation, health, political opinions, religious beliefs or criminal record.* |
| | |
| **What will happen to personal data once captured by your drone(s)? Will it be recorded or transmitted? How will it be transmitted, stored and otherwise processed and to what end? Describe any equipment – hardware and software, used to capture, record, transmit and store personal data.** | *Provide an overall picture of the data processing activities you will undertake. Think both if personal data is simply transmitted through a live feed and if it is recorded. What will happen to the data once it is in your possession? Pay special attention to describe what will happen to personal data you have captured.*<br><br>*If personal data is recorded, think about whether the data will be stored on the drone itself or whether it will be transmitted to other company facilities. Describe how data will be transmitted between equipment, e.g. WiFi, cable, SD cards, etc.*<br><br>*When describing the hardware and software, mention the model numbers and versions of software used and whether personal data will be stored on internal and/or networks. Mention all locations for personal data copies e.g. computers, private servers, cloud computing platforms. If there are multiple locations and copies of the data, mention all of them.* |
| | |

| | |
|---|---|
| **What kind of persons or organisations will personal data be shared with? Will personal data be shared with organisations outside of the EU or the EEA? Under what circumstances will personal data be shared with others, if at all? Consider your clients, if any.** | *Do you plan to share data after you have collected it? This can refer to using data processors to carry out specialised activities, to share data with a client or to make it public.*<br><br>*Describe the circumstances when personal data will be shared with others. For example, at what point in time will data be shared? What activities will you carry out prior to that? Will it be minimised, anonymised before sharing it with them?*<br><br>*Where you are using a data processor, you may ask them relevant questions for further information about how they will process and handle personal data. You can include this information here.*<br><br>*Include information about whether you have procedures for sharing personal data with public authorities, when requested and how they take place.* |
| | |
| **Describe how personal data will be disposed of. How long will personal data be maintained in a form that allows the identification of persons? Once the storage period has passed, how will personal data be disposed of?** | *Describe how long data will be maintained. This refers to personal data – as long as people captured are identifiable, the data is considered personal data. How long will such data be maintained?*<br><br>*At the end of a storage period, personal data should be disposed of by being erased or anonymised. Describe when and how that will happen.* |
| | |
| **Which personnel have access to the personal data? Describe the justification for them having access to personal data** | *Each person who has access to personal data you have collected should have a justification for such access, especially if this is not monitored. Justifications could be, for example, that this is necessary for the fulfilment of* |
| | |

| | |
|---|---|
| | *their professional duties or that they have a monitoring role to ensure compliance with relevant regulations and policies.* |
| **Has your organisation committed to complying with any relevant officially approved Codes of Conduct to help comply with data protection requirements?** | *If your company has subscribed to any Code of Conduct, which is it and how is it implemented in practice? Are there policies in place, is there an employee responsible for it? Mention especially whether this refers to any GDPR-approved Codes of Conduct.* |
| | |

## Step 3: Identify data protection risks

In the previous step you described how you plan on collecting, processing and disposing of personal data – the complete flow of personal data in your operation. In this step, the DPIA template will help you identify how data protection requirements apply to your data processing.

The questions will prompt you to consider risks resulting from your drone use or data handling practices. Once you have identified the privacy and data protection risks, you will be asked to choose the likelihood and severity of the risks to establish their potential impacts on individuals and on yourself and your partners. This includes:

- Likelihood - you will be asked to determine the likelihood of a risk materialising; and
- Severity - the severity of its impact if it does materialise. When assessing the severity of a materialised risk consider both the potential impacts for individuals on the ground, as well as for you and your business.

Measuring risk in this way can help you identify the full impact of the risks.

The ultimate goal of this step is to provide a full overview of how proportionate your interference with the personal data of individuals is. The larger quantity of personal data you process, the more parties you share it with, the more sensitive the personal data is, the greater the risks to individuals are likely going to be. It is, therefore, important to consider how your data processing complies with the GDPR in practice, step by step.

## Your lawful basis and purpose

| Risks arising with regard to your lawful basis and purpose | Guidance |
|---|---|
| **What is the purpose of your drone operation(s) and of the processing of personal data?** | *Describe what the purpose of your operation(s) is. Remember to define a clear and specific purpose. Ideally, your purpose would require that you use drones and personal data processing to fulfil them.* |
| | |
| **Is the purpose of your drone mission sufficiently specified, explicit and legitimate? Does the purpose necessitate the processing of personal data?** | *Before beginning your flight, you should have a clear purpose in mind. Consider the purpose you formulated in the preceding section.*<br><br>*Your purpose should either necessitate the processing of personal data or you should have the consent of individuals on the ground to capture them with your drone.* |
| | |
| **Are further purposes of personal data processing foreseeable at a later stage? If so, what may they be? Are they compatible with the original purpose or are they unexpected and unrelated to the original purpose?** | *Describe how you envision data collected being used if this goes beyond your initially planned purposes and data uses.*<br><br>*Keep in mind that any new uses of data which are not compatible with your original plan (i.e. which are different and unrelated) will have to be carefully considered and notified to people on the ground before you can rely on it for personal data processing.* |
| | |
| **What is the lawful basis for your drone processing personal data?** | *What is the lawful basis for you capturing and processing personal data? Identify the most appropriate lawful basis among the following (Article 6 GDPR):*<br>- *Individual consent, or*<br>*One of the following bases that necessitate the processing of personal data*<br>- *Legal agreement/ contract with the individual,*<br>- *Legitimate interests,*<br>- *Public interest or a public task,*<br>- *Vital interests of an individual,* |
| | |

| | |
|---|---|
| | - *Legal obligations.* |
| **Can you identify any potential weaknesses of relying on your chosen lawful basis?** | *Lawful bases differ in what they require, e.g. a contract, an explicit consent, a legal requirement falling on you. Do you fulfil all requirements of your lawful basis?*<br><br>*Is processing personal data truly necessary for the purpose of the flight?*<br><br>*Do you have documentary proof of everything required by your lawful basis/bases?* |

| **Assess risks related to your lawful basis for your drone operation(s)** |
|---|
| **Name / describe a risk you have identified** |
| |
| **What are the sources of this risk?** |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising*** |
| ***Identify the severity of a risk materialising*** |

+ Add further risks

| **Assess risks related to the purposes for personal data collection and processing** |
|---|
| **Name / describe a risk you have identified** |
| |
| **What are the sources of this risk?** |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising*** |
| ***Identify the severity of a risk materialising*** |

+ Add further risks

## Data minimisation

| Risks with regard to minimising your impact | Guidance |
|---|---|
| **How does the plan for your drone operation enable you to collect as little personal data as necessary for the purpose of the flight? How is processing of personal data and of sensitive personal data minimised?** | *Consider whether you have taken steps to minimise the collection, retention and processing of personal data to the minimum that is necessary for you to achieve your purpose.*<br><br>*Capturing personal data which is not necessary for your purpose can invalidate the lawful basis you rely on for capturing personal data.*<br><br>*Describe how personal data collection will be minimised during the flight. Consider what the impact of the following is:*<br>- *equipment and its capabilities,*<br>- *when sensors are engaged and when data is recorded,*<br>- *the flight path and time of flight of the operation.*<br><br>*For example, is flight near or over private or semi-private spaces limited? Is flight near sensitive spaces limited, e.g. churches, schools, kindergartens, political party headquarters, hospitals, police stations, prisons?* |
| ***Equipment:***<br><br>***Sensor engagement:***<br><br>***Data recording:***<br><br>***Flight path:***<br><br>***Time of flight:*** | |
| **Is the drone piloting team sufficiently aware of the context and precise purposes of the drone flight to allow them to carry out the flight and confine it to what is necessary?** | *The piloting team should be sufficiently informed of the environment in which they are operating, including where there are private, semi-private or potentially sensitive spaces, as well as whether there are any potentially sensitive areas near the drone operation, e.g. kindergartens, schools, religious buildings, political centres. This will allow them to carry out a flight in the best way possible, adapting if necessary.*<br><br>*The piloting team being aware of the purpose of the flight will also allow them to adapt to new* |
| | |

| | |
|---|---|
| | *circumstances, while fulfilling the mission.* |
| **Are any technical measures implemented to minimise the capturing and/or retention of unnecessary (personal) data? If so, what are they?** | *Examples of technical measures to minimise the data collected or retained could include automatic blurring or hiding of shapes of people by drone software, the erasure of any data captured beyond the parameters of a pre-determined flight path or its automatic erasure of data after a period of time.* |
| **Do you have a data retention procedure in place? If yes, describe the procedure briefly or where it can be found. How long is personal data maintained for and how is it discarded?** | *Does your data retention procedure include a reasonable retention period, considering the purpose of your operation?*<br><br>*Does it include flexible solutions, such as automatic erasure of personal data, administrator-initiated erasure and the possibility for legally authorised persons to override the retention period?*<br><br>*How and when will personal data be disposed of once it is no longer necessary? Would it be (and all its copies) erased or anonymised by removing any identifiable features from it?* |

| **Assess the risks of insufficient minimisation of personal data collected during flight(s)** |
|---|
| **Name / describe a risk you have identified** |
| |
| **What are the sources of this risk?** |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising*** |
| ***Identify the severity of a risk materialising*** |

+ Add further risks

| **Assess the risks of insufficient minimisation of data processed and retained after the flight(s)** |
|---|
| **Name / describe a risk you have identified** |
| |

| What are the sources of this risk? |
| --- |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising***  |
| ***Identify the severity of a risk materialising***  |

+ Add further risks

## Transparency of your operation

| Assess risks to transparency | *Guidance* |
|---|---|
| **Is the drone mission visible and transparent from the point of view of individuals on the ground? Is the drone visible? Is the launch site visible? Is the piloting team visible?** | *Visibility of a drone flight can help make your activities more transparent and bring some ease to the minds of people on the ground by letting them know that there is a drone operating and allowing them to know who to turn to for further information.*<br><br>*Is your drone visible, identifiable or marked in some manner, e.g. company logo?*<br><br>*Is the take-off point of your drone visibly marked and easily accessible? Consider the location and markings or signs which could point to the company's name.*<br><br>*Is the piloting team visible and accessible on the ground?* |
| **Are members of the piloting team trained to operate drones in a privacy-aware manner and how to interact with individuals on the ground?** | *This question seeks to ascertain how well prepared the piloting team are likely to be when it comes to privacy-aware drone piloting and responding to questions and concerns by individuals on the ground. Would they be able to refer individuals to further appropriate information resources?* |
| **How will people on the ground and local businesses be informed about your drone flight before or during the flight?** | *Describe what kind of information materials you will use to inform individuals in the area of your operation.*<br><br>*Ideally, individuals on the ground should be aware of:*<br>- *the identity and contact details of the data controller or the named Data Protection Officer (DPO)*<br>- *the purpose and lawful basis for the processing*<br>- *the sharing of personal data with third parties – categories of recipients,* |

| | |
|---|---|
| | *transfers to third countries outside the EU or the EEA and the circumstances,*<br>- *data retention period,*<br>- *the rights individuals have and how they can exercise them,whether their data is processed through automated decision-making.*<br><br>*Describe also what channels will be used to inform individuals. Describe:*<br>- *channels of communication used,*<br>- *any visual details that distinguish your drone during flight and when recording,*<br>- *comprehensive and up-to-date information documents, e.g. Privacy Notice specific for this mission,*<br>- *on-the-ground information points you have set up in the area of your operation.* |
| **Are the communication channels which you have chosen to use to inform people of your activities before and during the drone flight(s) likely to be effective? Are they clear, understandable and will they reach their intended audience?** | *Considering the particular location in which you will operate and the kind of people who are likely to be there or nearby, do you believe the communication channels you have chosen are likely to be effective in informing people of your activities?*<br><br>*Will the right people receive the information? Is access free and easy?*<br><br>*Will they receive sufficiently detailed information – e.g. the identity of the operator and contact information, purpose of the operation, the legal basis or legitimate interests you pursue, the nature, dates, times, duration and locations of flights, the categories and types of data you collect, the processing of data, whether personal data is shared with third parties, what rights individuals have.* |
| | |

| Assess the risks of insufficient transparency before, during or after the flight(s) |
| --- |
| **Name / describe a risk you have identified** |
| |
| **What are the sources of this risk?** |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising***  |
| ***Identify the severity of a risk materialising***  |

+ Add further risks

## Sharing personal data with third parties

| Assess risks to sharing data | *Guidance* |
|---|---|
| **Do you have a legal agreement clarifying your relationship and allocation of responsibilities with any third parties with whom you will share data? Please describe them and, specifically, focus on how personal data will be shared and processed.** | *Provide information about the contracts, code of conduct, certifications and other documents which lay out the legal relationship between you and third parties, based on which you share personal data with them.*<br><br>*Describe all bodies that you plan on sharing personal data with:*<br>- *data processors, e.g. cloud computing service providers*<br>- *data controllers, e.g. clients that have hired you*<br>- *joint data controllers that you process personal data with.*<br><br>*Describe under what circumstances personal data will be shared with such third parties – what the duration, scope, purpose of the processing will be, whether data will be shared before or after being anonymised.* |
| **Once shared with third parties, will personal data be processed for other purposes than the originally intended purpose for data collection? If yes, what are they and are potentially impacted individuals aware of or can expect these purposes?** | *Individuals need only be aware of the purposes for data processing of third parties where it is their personal data that is being shared and processed. If data relating to them have been deleted or anonymised in another manner, this will no longer be necessary.* |
| **Will any of the parties you share personal data with be located outside the EU or the EEA? If so, are there legal measures to ensure that the personal data is protected, such as an adequacy decision by the European Commission, an international commitment by the third country, contractual clauses or individual consent?** | *Name each country outside the European Union or the EEA to which personal data is transferred and state what adequate protections you rely on to carry out the transfer, e.g. the country has been recognised as providing adequate protection, you use Commission-approved model contract clauses, etc.* |
| **Do you have written policies in place to disclose captured data to competent authorities? Please describe them.** | *Do these policies inform your employees under what* |

| | |
|---|---|
| | *circumstances to comply with such requests and what information to provide in response. Do they cover issues such as which authorities have access to data, how information should be handled and disclosed, as well as that data recipients become the new data controllers?* |

| **Assess the risks when sharing data with third parties, e.g. processors, clients, authorities** |
|---|
| **Name / describe a risk you have identified** |
| |
| **What are the sources of this risk?** |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising***  |
| ***Identify the severity of a risk materialising***  |

+ Add further risks

## Ensuring individual rights and freedoms in practice

| Ensuring individual rights and freedoms | Guidance |
|---|---|
| **How can individuals whose personal data you process (data subjects) exercise their right of access?** | *How can individuals approach you? What information do you request from individuals when they make a request? Are there any associated costs for individuals to cover? What information and when do you respond to them with?*<br><br>*In the GDPR, individuals have the right to access their personal data. This means they have the right to:*<br>- *know whether you are processing their personal data,*<br>- *know what kind of personal data is processed, how, who it is shared with,*<br>- *know what the data retention period is,*<br>- *receive a copy of their data.* |
| **How can individuals exercise their right to data portability?** | *How can individuals approach you? What information do you request from individuals when they make a request? Are there any associated costs for individuals to cover? What information and when do you respond to them with?*<br><br>*Where personal data is processed on the basis of individual consent or a legal agreement with an individual, people have the right to data portability. Individuals have the right to receive a copy of their personal data in a readable format or to have such data transferred to a third party.* |
| **How can individuals exercise their right to rectify and erase their personal data?** | *How can individuals approach you? What information do you request from individuals when they make a request? Are there any associated costs for individuals to cover? What information and when do you respond to them with?* |

| | |
|---|---|
| | *Individuals have the right to ensure their personal data is up-to-date and accurate – the right to rectify. Individuals also have the right to have their data erased. These rights apply in a set of circumstances, according to the GDPR. Do you have a policy in place to determine when to comply with their requests?* |
| **How can individuals exercise their rights to object to processing or restrict processing?** | *How can individuals approach you? What information do you request from individuals when they make a request? Are there any associated costs for individuals to cover? What information and when do you respond to them with?*<br><br>*Individuals have the right to permanently (object) or temporarily (restrict) prevent the processing of their personal data. There are limits to when individuals have this right pursuant to the GDPR. Do you have policies in place to determine when you should comply with this right?* |
| **Do drone pilots and other staff receive ongoing training in how to respect data protection during a flight and subsequently, when handling data?** | *Staff that operates within your business premises has to remain informed of how to handle data in a responsible manner and how to respond to privacy and data protection requests from individuals captured by the drone operation(s).*<br><br>*As a key part of the data collection process, pilots should also have a keen understanding of privacy and data protection considerations as they play a role in the drone operation.*<br><br>*Do they know about relevant legislation, best practices in flying drones and privacy and data protection considerations during drone operation?* |

| | |
|---|---|
| **Are the procedures for individuals to exercise their rights quick, effective and easily accessible from the point of view of individuals? Please elaborate.** | *The procedures you have put in place have to allow individuals to easily and effectively exercise their rights, where they have such rights. Are your internal procedures proportionate with regard to the burden they place on individuals, including any costs or needs to prove identification, as well as the time frames you have set?* |
| | |
| **Are there auditing mechanisms within your organisation to ensure the compliance of employees with these policies and procedures? If yes, how do these mechanisms function?** | *This question seeks to ascertain whether there are any internal audits or oversight mechanisms that ensure employees comply with company procedures, practices and commitments in practice.* |
| | |

| **Assess the risks related to individuals exercising their rights and freedoms** |
|---|
| **Name / describe a risk you have identified** |
| |
| **What are the sources of this risk?** |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising*** |
| ***Identify the severity of a risk materialising*** |

+ Add further risks

## Data accuracy and security

| Assess risks to data security | Guidance |
|---|---|
| **How is the (cyber-)security of the collected personal data ensured within your organization during collection (during flight), during storage and when sharing with other bodies (during transfers)?** | *What security measures are in place to protect personal information from loss, unauthorised access, use, modification, disclosure or other misuse? Do you employ one or more of the following:*<br>- *security or data privacy standards or recognised certificates,*<br>- *technical measures to protect data, e.g. through encryption and access controls,*<br>- *internal security policies and practices,*<br>- *training for staff and employees.*<br><br>*Do you have up-to-date list of personnel who have access to personal data, e.g. footage that has not been anonymised?* |
| **Do you have procedures or practices in place to ensure the accuracy and security of drone equipment prior to flights taking place?** | *Drone equipment and software can sometimes be inaccurately calibrated or have technical defects. This could result in inaccurate data collection. This may raise data protection issues when it captures personal data inaccurately.*<br><br>*Through procedures you could, for example, ensure:*<br>- *the accuracy of payload sensors,*<br>- *that the drone has up-to-date information of the flight area,*<br>- *that the drone's features and settings are appropriately tailored for the mission.* |
| **Do you have any internal policies to handle situations of a data breach – unauthorised access to personal data by internal or external persons?** | *You do not have to describe details of your procedure, such as internal phone numbers or emails, but you should lay out your procedure in general terms.* |

| | |
|---|---|
| | *Are personnel aware of how to act in case of a data breach? Have employees received training in that?* |

| **Assess the risks of insufficient data accuracy** |
|---|
| **Name / describe a risk you have identified** |
| |
| **What are the sources of this risk?** |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising*** |
| ***Identify the severity of a risk materialising*** |

+ Add further risks

| **Assess the risks of insufficient data security** |
|---|
| **Name / describe a risk you have identified** |
| |
| **What are the sources of this risk?** |
| |
| **What are the impacts of this risk on individuals?** |
| |
| **What are the impacts of this risk on your company and/or your clients?** |
| |
| ***Identify the likelihood of a risk materialising*** |
| ***Identify the severity of a risk materialising*** |

+ Add further risks

## STEP 4: Solutions to minimise data protection risks

This section helps you identify solutions to respond to the risks identified in the preceding section. Solutions in general can include:

- technical safeguards – security measures, technical means to minimise data collected or held, or protect it from unauthorised access,
- procedural safeguards – internal guidance for behaviour and handling data, data breach responses, as well as structures ensuring co-workers comply with internal procedures.

This section will highlight all risks you have previously identified and prompt you to consider, in a systematic manner, what safeguards and solutions you could implement to respond to their underlying reasons.

In the sections below, you will find a set of guiding questions and some suggested solutions to safeguard personal data which you can implement in practice. This list is intended to help guide your thinking about solutions to protect privacy and personal data of individuals and is not exhaustive. You should decide by yourself what safeguards are available to you and your company and choose the most appropriate ones for the operation(s) in question.

You can consult other resources to help you identify relevant safeguards, including the DroneRules PRO e-learning course and the Privacy Code of Conduct, which encompasses a set of best practices.

Add as many fields as necessary to the tables below to describe all safeguards you believe may be appropriate.

## Your lawful basis and purpose

What safeguards can you implement to tackle the risks that you identified in the above section titled "Your lawful basis and purpose"? Have you carefully considered, planned and documented all necessary details regarding your lawful basis and the purpose of your activities, at least as far as personal data collection is concerned? How can you prevent risks from materialising or mitigate them to the greatest extent possible? Could planning and documenting practices, staff trainings and/or involving experts and/or senior management help you mitigate these risks?

| **Risk and risk severity** ***(automatically generated field)*** | **Proposed solution(s)** | **Result**[27] ***(choose as appropriate from the drop-down menu)*** | **Evaluation**[28] ***(choose as appropriate from the drop-down menu)*** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[27] What is the result of this safeguard? Is risk eliminated, reduced or accepted?
[28] What is your evaluation of the risk after the implementation of the safeguard? Is the final impact on individuals a justified, compliant and proportionate response to the aim of your operation?

## Data minimization

What were the risks you identified in the "Data minimization" section above? Can any of these risks be eliminated or mitigated through careful planning, technological means, procedures or internal policies? Every choice you make – from your equipment, to the time and place of your flight, to the processing and erasure of the collected data, should be made in a way to minimise your impacts on the privacy of individuals and collect as little personal data as possible. How can you achieve that and minimise your impact on the privacy and personal data of individuals at each of these steps and ensure that things go according to plan?

| **Risk and risk severity** ***(automatically generated field)*** | **Proposed solution(s)** | **Result**[29] ***(choose as appropriate from the drop-down menu)*** | **Evaluation**[30] ***(choose as appropriate from the drop-down menu)*** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[29] What is the result of this safeguard? Is risk eliminated, reduced or accepted?
[30] What is your evaluation of the risk after the implementation of the safeguard? Is the final impact on individuals justified, complaint, proportionate response?

## Transparency of your operation

When you were filling out the "Transparency of your operation" section above, did you identify any risks of your operation, resulting from you not taking steps to be transparent or from mishaps with regard to the steps you were planning? How can you ensure that your operation is as transparent as possible from the point of view of people on the ground? What kind of communication channels and information materials could you use? Who should you inform of your activities, what should you tell them and what is the best way to do that?

| **Risk and risk severity** ***(automatically generated field)*** | **Proposed solution(s)** | **Result**[31] ***(choose as appropriate from the drop-down menu)*** | **Evaluation**[32] ***(choose as appropriate from the drop-down menu)*** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[31] What is the result of this safeguard? Is risk eliminated, reduced or accepted?

[32] What is your evaluation of the risk after the implementation of the safeguard? Is the final impact on individuals justified, complaint, proportionate response?

## Sharing personal data with third parties

In the "Sharing data with third parties" section above, what weaknesses did you identify with regard to your practices to sharing personal data? Are you certain that you are complying with your legal obligations when sharing personal data? Have you informed individuals that you will share their data further or do you have another legal reason to do so? Is the security and privacy of data guaranteed even in the hands of third parties? Can you use legal agreements, staff training, auditing policies or other means through which to ensure this?

| **Risk and risk severity** *(automatically generated field)* | **Proposed solution(s)** | **Result**[33] *(choose as appropriate from the drop-down menu)* | **Evaluation**[34] *(choose as appropriate from the drop-down menu)* |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[33] What is the result of this safeguard? Is risk eliminated, reduced or accepted?
[34] What is your evaluation of the risk after the implementation of the safeguard? Is the final impact on individuals justified, complaint, proportionate response?

## Ensuring individual rights and freedoms in practice

Does your organisation ensure that individuals can easily and efficiently exercise their rights when you process their personal data? Is your staff well-informed and trained on how to act when responding to data subject access requests? Are there internal procedures, policies and trainings to facilitate this? How often should staff be trained and what kind of information should they be aware of? Are your policies accurate and up-to-date? How do you ensure that your employees comply with these procedures? Do you keep an up-to-date documentary archive of your operations and all privacy and data protection related decisions you have made with regard to them? Is there someone responsible for that?

| **Risk and risk severity** *(automatically generated field)* | **Proposed solution(s)** | **Result**[35] *(choose as appropriate from the drop-down menu)* | **Evaluation**[36] *(choose as appropriate from the drop-down menu)* |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[35] What is the result of this safeguard? Is risk eliminated, reduced or accepted?
[36] What is your evaluation of the risk after the implementation of the safeguard? Is the final impact on individuals justified, complaint, proportionate response?

## Data accuracy and security

What risks did you identify in the "Data accuracy and security" section above? Is your data sufficiently protected against unauthorised or unlawful processing and against accidental loss, destruction or damage? What tools do you have at your disposal and how do you use them to guarantee it is secure? Can you adhere to security standards, codes of conduct, etc.? Can you implement technical measures to ensure data accuracy and security or develop internal policies and dedicate employees for this task? What kind of criteria do you use when choosing the equipment, hardware and software used in your company and can that be improved?

| **Risk and risk severity** ***(automatically generated field)*** | **Proposed solution(s)** | **Result**[37] ***(choose as appropriate from the drop-down menu)*** | **Evaluation**[38] ***(choose as appropriate from the drop-down menu)*** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[37] What is the result of this safeguard? Is risk eliminated, reduced or accepted?
[38] What is your evaluation of the risk after the implementation of the safeguard? Is the final impact on individuals justified, complaint, proportionate response?

## Step 5: Results of the DPIA

This section of the DPIA provides you with a finalised list of all identified risks and safeguards. This section helps you create an easy to consult checklist that can be used by anyone conducting the drone flight and the subsequent personal data processing activities. These results will remind operators and relevant actors within your organisation of the safeguards they need to implement to support a privacy-by-design approach to drone missions of the organisation, as well as being a privacy reference sheet for pilots and staff involved in the mission.

### Summary of drone mission(s)

*Please complete the fields below*

| | | |
|---|---|---|
| **What is the drone operation being undertaken:** | | |
| **Purpose of drone operation(s):** | | |
| **Drone operation location and time:** | Location: | Time: |
| **Drone operation lawful basis/bases:** | | |
| **Types of data collected:** | | |
| **Clients involved, if any:** | | |

### Record of DPIA outcomes

*This section will be partially automatically generated based on the information input in the foregoing "Step 4: Solutions to minimise privacy and data protection risks".*

| **Risk** ***(automatically generated field)*** | **Approved solution (s)** ***(automatically generated field)*** |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Solutions reviewed by …… on ……
(name) (date)

Solutions approved by …… on ……
(name) (date)

## Further resources to consult

If you would like to know more about PIAs or DPIAs, there are a variety of information resources available online.

**Legal texts**

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

**DPIA guidance documents**

Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248, 4 April 2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

Bitkom, "Risk Assessment & Data Protection Impact Assessment: Guide", Berlin, September 2017. https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Data-Protection-Impact-Assessment.html

Information Commissioner's Office, "Data Protection Impact Assessments (DPIAs)", in Guide to the General Data Protection Regulation (GDPR). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

92. Conference of the Independent Data Protection Authorities of the Bund and the Länder (Germany), "The Standard Data Protection Model: a concept for inspection and consultation on the basis of unified protection goals", Version 1.0, Kühlungsborn, 9-10 November 2016. https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf

Commission nationale de l'informatique et des libertés (CNIL), "The open source PIA software helps to carry out data protection impact assessment", 31 May 2018. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

**PIA guidance documents**

Information Commissioner's Office, "Conducting privacy impact assessments: code of practice", 20140225, Version 1.0, February 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Information Commissioner's Office, "Privacy Impact Assessment: Executive Summary". https://ico.org.uk/media/about-the-ico/consultations/2047/pia-executive-summary.pdf