

Privacy and data protection case study

Below you will see some of the main privacy and data protection issues that could arise in this situation and tips/safeguards for how to avoid them.

11 - RESCUE MISSION



You are a national authority wanting to use drones on rescue missions during an emergency or after a natural or humanitarian disaster. For example, you deploy a drone equipped with thermal imaging, a mobile phone signal sensor and GPS capabilities to search for hikers lost in the woods.

Privacy

Transparency, visibility and accountability: Drones can remain undetected by individuals on the ground, who may not be aware that a drone is in operation or that it is collecting their personal data. This is especially true in the forest where trees could obstruct the visibility of the drone. Even if people notice it, they are unlikely to be able to identify the operator or the specific mission that is being undertaken.

Bodily privacy: This can be threatened when drones are fitted with equipment that, aside from visual information, has also thermal (e.g. thermal sensors) or other capabilities, e.g. facial recognition, biological and chemical sensors.

Privacy of location and space: Persons have the right to move freely without being identified, tracked and monitored, even in public spaces. Use the drone to look for and pursue specific people only in emergency circumstances.

DATA PROTECTION

Remember that there are special requirements that apply whenever people whose information or images you collected can be identified (making it their personal data). Keep in mind that sometimes it may be possible to identify people also from the context – location, house numbers, car registration numbers, time of day, etc.

Lawfulness, fairness, transparency: Your collection and processing of personal data must be lawful, based on one of the options laid down by EU law. It must be fair, meaning that it must not cause any harm to the individuals. It must also be transparent – people have to know if their images have been captured, by whom and why.

Purpose limitation: People have the right to know exactly for what purpose their data is collected and, once you inform them of the reason (security, safety and rescue missions), you cannot use their data for a different incompatible purpose (e.g. examining visitors to the park for marketing purposes) without informing them again and ensuring your actions are lawful (see above).

Storage limitation: You should not keep the footage of people in a manner that would allow their identification for longer than necessary to achieve your legitimate purpose. However, consider if there are other legitimate reasons to keep the information, for example for insurance needs, archive necessities or other legal requirements.

Integrity and confidentiality: Where you have footage of identifiable people, you should make sure that that data is stored in a secure and protected manner. It should be protected from unauthorised access by both third parties, as well as your own employees.

Accountability: Remember that, if you collect personal data and can choose what to do with it, you will be accountable if you don't follow any of these principles.

SAFEGUARDS

TIPS - *Consider how best to inform persons that they may be subject to surveillance in the event of a rescue mission, e.g., have signs at the entrance to a park / walking path and add information on the website of the location, if there is one.*

TIPS - *Do not fly too close to persons so as to make them feel uncomfortable or cause them harm.*

TIPS - *You must act in accordance with the applicable rules of law. Take time to understand those. Since some of the information you may collect, for example the thermal body images of the people in the park, may be considered sensitive data, special rules may be applicable.*

TIPS - *Once the mission (i.e. the legitimate purpose) is finished, discard data that you collected, unless it is necessary for subsequent investigations or legal actions constituting a legitimate purpose. If any data needs to be stored, ensure that personal data are stored and processed securely and protected from disclosure and unlawful intrusion. Only store the minimum personal data necessary.*

TIPS - *Do not share data on identifiable persons with third parties without those persons' consent or without another legal obligation requiring you to do so.*

TIPS - *Consider taking steps, such as blurring as soon as possible to minimise the amount of personal data collected from people inadvertently captured by the sensors of the drone. However, pay attention not to remove information that may be necessary at a later stage for investigations, insurance purposes or pursuant to other legal requirements.*

TIPS - *Individuals recorded should have a right to access the material concerning their own personal data and to request that the data controller delete that material. They should be informed of this right. However, pay attention to any other legal requirements you may be subject to.*

TIPS - *Be aware who the data controller and processor is, especially if you are carrying out this activity together with another company. Remember that data controllers and data processors are subject to various legal obligations in the EU.*

