

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.

8 - PROVIDING INTERNET OR OTHER WIRELESS SERVICES



You are a private company that wants to use drones to disperse some kind of wireless signal to, for example, remote areas. You are providing access to different kinds of communication services that run through your drone. By doing this, you may inadvertently also collect personal data such as the IP addresses of computers or devices connected to your network, as well as the traffic passing through them.

Privacy

Transparency, visibility and accountability: Drones that disperse communication signals tend to be large enough to be noticeable. Even if people are aware of the presence of the drone, however, they may still not be aware what kind of personal information the drone may collect, nor who exactly operates it. Generally, people should be aware of who and why is operating the drone.

Privacy of personal communication: Individuals have the right to privacy of their communication. The interception, recording or access to their private communication is forbidden. If you are offering Internet or other wireless communication services through your drone, this aspect of the right to privacy may be jeopardized if the transfer of their communication through your platform is not secure and private.

Chilling effect: People may not be aware of exactly what the drone is doing or whether or not it can collect visual data. If they feel like they are being surveyed, they may change their behaviour. This could apply also with regard to their online behaviour, if they believe their use of the network could be monitored.

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 which of their personal data has been collected, by whom and what it will be used for.

Purpose limitation: People have the right to know exactly for what purpose their data is collected and, once you inform them of the reason (wireless communication), you cannot use their data for a different incompatible purpose (e.g. advertising) without informing them again and ensuring your actions are lawful (see above).

Data minimisation: You should collect the minimum amount of personal data possible for your legitimate purpose.

Accuracy: You should ensure that the personal data that passes through your platform is accurate and up-to-date. If there are inaccuracies, they should be deleted or fixed without delay. **Storage limitation:** You should not keep any personal data in a manner that would allow a person's identification for longer than necessary. IP addresses can lead to the identification of people too.

Integrity and confidentiality: You should make sure that any data on the drone platform is secured and protected both from unauthorised access and from possible file corruption. The data should be protected both by third parties and 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 informing the people living in the area of the various channels or functions of the drone, what it can and cannot do, the information it collects and what it uses it for. Give your own contact information to answer any questions the people may have.

TIPS – Ensure that people are informed of the way their data will be processed when they use the wireless network from the drone, e.g. by showing them a message when they connect to the wireless services. Also, inform them of their rights, including their right to receive access to all their data and to request that it be deleted.

TIPS - Implement strong encryption systems in your drone to ensure the security of communication that passes through it and to protect the files from being corrupted. Store any data in a secure manner and ensure that it is not stored for excessive lengths of time. **TIPS** – Only collect and store data that is relevant or necessary for the purposes for which it is being collected, for the task you are carrying out, e.g. communication facilitation. Collect the minimum amount of data possible.

TIPS – Consider taking anonymising steps as soon as possible, e.g. giving users pseudonyms, scrambling and encrypting data end-to-end, etc. to minimise the amount of personal data collected. Note that pseudonyms may also be considered personal data if they may be linked to identifiable persons.

TIPS - Do not share data on identifiable persons with third parties without the persons' consent.

TIPS – Be aware who the data controller and processor is in this case, 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.

