Saba Elizbarashvili*

Processing of Personal Data Through the Use of Drones (Review of International Standards and Compliance with Georgian Legislation)

Video recording represents one of the most pervasive forms of data processing. The advancement of modern technologies, including drone aerial photography systems, has introduced a host of new challenges concerning the protection of personal data. The accessibility and user-friendliness of drones enable individuals to process personal data of a considerable number of subjects, thereby significantly increasing the risk of violating the provisions outlined in Georgia's existing and forthcoming laws "on Personal Data Protection". The paper examines the standards established for the legality of drone data processing and offers relevant recommendations to data controllers.

Keywords: *Personal data protection, Personal data processing, Modern technologies, Video recording, Drone.*

1. Introduction

With the rapid advancement of technology, which includes drones, and the integration of smart systems, the potential for data collection reaches an almost boundless scale. GPS technology, frequently a built-in feature of drones, enables the tracking and recording of the drone's location as well as that of any surveillance targets.[1] In addition, the drone can be equipped with a sound recording device, as well as simple, night vision, and/or thermal imaging (thermographic) cameras that can detect the location of a person based on body heat. The drone can also be equipped with 3D scanners, as well as WiFi and/or Bluetooth devices, and recognition systems for mobile devices,[2] which provide the ability to track a person's location via their mobile phone. The use of such systems by drones can have a significant negative impact on an individual's data protection and privacy rights.

Advanced surveillance technologies can integrate a drone's high-quality audiovisual recording and storage capabilities with data analytics tools like facial recognition software, gait analysis, and other biometric assessment systems, which enables targeted surveillance of individuals.[3] Furthermore, the size and maneuverability of drones afford the capability to observe, track, and follow targets from a considerable distance without the monitored

* Master of law at Ivane Javakhishvili Tbilisi State University; Lawyer of the Legal Department at Personal Data Protection Service of Georgia.

[1] *Tarr T., Tarr J. A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1.

[2] Spanish Data Protection Agency, Drones and Data Protection, 2019, 1, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

[3] *Tarr T., Tarr J. A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1.

individual being aware of such surveillance.[4] Therefore, a key challenge with drone use is the limited awareness of the data subject which, on the one hand, is manifested in the lack of information about data processing itself and on the other hand in the identity of the data controller (drone operator).[5]

Personal data is defined as "any information relating to an identified or identifiable natural person",[6] drone operators that record or/and process images, video, voice, biometric data, geolocation, or telecommunications data related to an identified or identifiable individual should be considered as data controllers, (except in cases where the drone is used solely for household or personal purposes).[7] Therefore, in cases where drones are used under the conditions mentioned above, drone operators, as data controllers, are subject to both the General Data Protection Regulation (GDPR) and the rules established by the Georgian Law on Personal Data Protection.

It should be noted that, taking into account the European practice, excluding national or international legislation on personal data protection, various types of specialized documents may address issues related to personal data protection in the context of drone usage. These documents may include manuals prepared by supervisory bodies, internal regulations governing civil aviation, and documents developed by the European Union in this field. This article discusses the main data protection standards and recommendations in the process of using drones, including the structure, content and goals of individual documents regulating the issue.

2. Drone Operator/Data Controller Obligations

Regarding the issue of personal data protection in the process of drone use, we find essentially similar approaches across Europe. In particular, special attention is focused on the obligations of the drone operator and the need to ensure proper data protection guarantees. Among these, notable obligations include transparency, informing the data subject, ensuring data security, and practicing data minimization. Furthermore, it is essential to consider data protection standards, such as Data Protection by Design and by Default, and to prepare an impact assessment on data protection when developing a new product or service.

2.1. Transparency and Obligation to Inform the Data Subject

Article 15 of the Law of Georgia "On Personal Data Protection" outlines the obligatory procedure for disclosing information to the data subject. This requirement holds particular relevance in drone-related data processing scenarios, as in most cases, the data subject remains unaware of their data being processed and the identity of the data controller.

[4] Ibid.

[5] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36.

[6] The Law of Georgia on "Personal Data Protection", 5669-rs, 28/12/2011, art. 2, sub-para. "a".

[7] In the case of using a drone solely for family, economic, or personal purposes, the direct operation of the drone by an individual may be exempt from obligations established by personal data protection legislation. However, if the data obtained as a result of such operation is subsequently processed (such as distributing photo, video, or audio material on social networks), the requirements set forth by legislation will apply as standard.

In many instances, due to the large number of data subjects, it becomes challenging, if not impossible, to individually inform all subjects within the drone's filming area (e.g., in a stadium, on the street, etc.). Accordingly, drone operators are tasked with finding "innovative" methods to provide information to individuals whose personal data is processed as a result of drone use. In cases where it is particularly challenging or requires a disproportionately large effort, the data controller should endeavor to inform the subjects through alternative means, which can be expressed, for example: officially registering the drone with the civil aviation authority, displaying appropriate signage in the area of drone operation, publishing a privacy notice on the data controller's website, or presenting privacy notice through alternative channels.[8]

It is crucial for the data subject to easily discern the identity of the drone operator or data controller.[9] Therefore, to facilitate the identification of the responsible party controlling the drone, it is advisable for both the drone and its operator to remain within the field of vision of the data subject.[10] To enhance visibility, the drone operator may choose to wear easily identifiable attire. Additionally, it is advisable for the operator to be prepared to furnish requested information to interested individuals via a QR code. This QR code can direct the data subject to a website link containing details about the personal data protection policy.[11] Furthermore, to ensure adherence to the principle of transparency, the drone should be equipped with an appropriate signaling system, such as a flashing light or audible sound, to alert the data subject to the ongoing recording by the drone.[12]

In each specific case, it is essential to assess the most effective method of informing the data subject, whether it involves placing information signs or cards in the vicinity of the drone's operation, publishing information on social media or in print media, distributing informational brochures, displaying posters, or other suitable means.[13] The main aim is to ensure that the data subject is informed about the data processing activities, including details about the data controller, the purpose of processing, and the rights of the data subject.

2.2. Data Minimisation Principle

According to Article 4 "G" of the Law of Georgia "On Personal Data Protection", data may only be processed to the extent necessary to achieve the relevant legal purpose. Additionally, the data must be adequate and proportionate to the purpose for which they are processed.

[8] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36.

[9] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 22, 32, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

[10] The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].

[11] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[12] Ibid, 5.

[13] Spanish Data Protection Agency, Drones and Data Protection, 2019, 4, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

The principle of data minimization is particularly crucial in the process of data processing using a drone. On one hand, in some cases, the number of subjects involved in such data processing can be particularly large, which can exacerbate the threat to the rights of the data subjects. However, on the other hand, various technical facilities make it relatively easy to achieve the minimization of drone data.

Minimizing interference with human privacy and data protection rights can be achieved by planning and considering the following issues/actions in advance: 1. specific flight route, 2. appropriate type of drone and its equipment, 3. management of collected data.[14]

The data collection and storage systems integrated into the drone can be configured by default to prevent the collection and processing of unnecessary amounts or types of data. This can be achieved, (for example, by automatically depersonalizing the data, such as blurring the images of individuals moving in the area captured by the camera),[15] to avoid indiscriminate or excessive data processing, the drone operator must adhere to the principles of data minimization, as well as consider options for anonymization and pseudonymization.[16]

To adhere to the principle of data minimization, the data collection systems installed on drones should feature on-off functionality as needed, and the captured visual angle of the frame should be limited to the specific purpose of data processing (for example, if the drone is being used to inspect a particular section of a damaged roof, there is no need for a 360-degree angle of view).[17]

To minimize data, it is advisable for the drone operator to limit the number of people and identifiable objects (eg, a license plate) in the frame as much as possible. This goal can be achieved by conducting flights during times of the day when the lowest concentration of people is observed in a specific area. Additionally, it's preferable to conduct video/audio recording or photography only at specific moments when necessary, rather than throughout the entire flight.[18]

To prevent such invasive photo or video recording, which grossly violates people's privacy, the drone operator must be aware of the technical capabilities of the drone being used. In particular, the operator should be aware of how well the drone records images, the extent to which it can zoom in on a shot (known as "zoom"), and whether it is technically possible to start and stop filming during flight.[19] To gain a better understanding of this information and become acquainted with the drone's capabilities, it is advisable for the operator to conduct test flights in a controlled environment before flying in public spaces.[20]

---

[14] *Tarr T., Tarr J. A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 3.

[15] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4-5. <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[16] Personal Data Protection Service, Worldwide Practice, June/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].

[17] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[18] Spanish Data Protection Agency, Drones and Data Protection, 2019, 3, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

[19] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 21, 32, < https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

[20] Aerialworx, The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].

Additionally, any data beyond the scope of the intended processing and with no need to store, should be promptly deleted.[21]

2.3. Data Security Requirement

Article 17 of the Law of Georgia "On Personal Data Protection" outlines the obligation of data security. Specifically, it states that "the data controller is obliged to implement organizational and technical measures to ensure the protection of data from accidental or unlawful destruction, alteration, disclosure, extraction, or any other form of unlawful processing, as well as from accidental or unlawful loss." Various security challenges may arise during data processing using drones. Therefore, it is the responsibility of the drone operator to implement appropriate safety measures.

First of all, it is important to determine if the drone is connected to any other systems. In such a case, appropriate safety measures should be taken. In addition, the drone operator must ensure that all data collected is stored securely, which may be achieved by encrypting the stored information or employing other methods to restrict access to it. This is particularly important when the drone is flown over long distances, beyond the pilot's field of vision, or in the event of a drone crash, which increases the risk of both the device and its data being lost or stolen.[22]

It is the responsibility of the data controller to take the necessary technical and organizational measures to ensure the security of data processing using drones. Therefore, the data controller should pay special attention to the technical features that the drone is equipped with and which aim to ensure safety in the process of data collection and storage. Among these considerations, the drone operator should verify where the photo/video material captured by the drone is stored—whether it's on the device itself, a portable memory card, or in a cloud-based system. To mitigate potential risks, the data controller must implement suitable measures, such as encrypting the data before transmitting it to the cloud system.[23]

2.4. "Data Protection By Default and By Design"

Article 26 of the new law of Georgia[24] "On Personal Data Protection" establishes the priority of maximal data protection coverage as the default method automatically employed before considering an alternative approach when developing a new product or service (Data Protection by default and by design), a concept that mirrors Article 25 of the GDPR.

According to this article, considering new technologies, implementation costs, the nature, the extent, context, and purposes of processing, as well as the anticipated risks to the rights and freedoms of the data subject and the principles of data processing, the data

[21] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023. Point 25, 33, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

[22] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 36-37, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf> [04.09.2023].

[23] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].

[24] Law of Georgia "On Personal Data Protection", 3144-XIms-Xmp, 14/06/2023.

controller must take suitable technical and organizational measures (including pseudonymization and/or others) both in determining the means of processing and directly during the processing itself. The adoption of these measures should ensure the effective implementation of data processing principles and the integration of protection mechanisms in the data processing process to safeguard the rights of the data subject. Additionally, the data controller, when determining the volume and extent of data processing, storage periods, and access to data, must ensure that technical and organizational measures are taken to automatically process only the amount of data necessary for the specific purpose of processing. These measures should be implemented in a manner that grants access to only the minimum amount of data automatically to an indefinite number of individuals until an authorized alternative approach is selected. Thus, on one hand, the drone manufacturer must integrate mechanisms that minimize the data collected by the drone during the production process. In producing drones, it is essential for the manufacturer to operate with a foundation of respecting human rights to safeguard the privacy of subjects.[25]

On the other hand, the drone operator must consider data protection issues when selecting the appropriate drone for a specific task, planning the flight route, and developing data processing procedures.[26]

It is the responsibility of the drone operator, as a data controller, to ensure that the drone system he intends to use complies with the high priority data coverage provided for in Article 26 of the Law (ensuring that the drone has technical capabilities such as recording and storing data only when it climbs to a certain height[27] or reducing the clarity/resolution of the photo to the minimum necessary to achieve the purpose of data processing [28] among other measures).

2.5. Data Protection Impact Assessment

According to the first paragraph of Article 31 of the new Law of Georgia "On Personal Data Protection," if during data processing, considering new technologies, the category and volume of data, as well as the purposes and means of data processing, there is a high probability of a threat to the violation of basic human rights and freedoms, the data controller is obliged to conduct a data protection impact assessment in advance. Impact assessment is not a one-time process, rather, it is ongoing, especially when the data processing measure is dynamic and characterized by periodic changes.[29]

Based on the reasoning developed in the previous chapters, it is evident that in many cases, data processing using a drone may reach the thresholds outlined in the

[25] Privacy by Design Guide, Resource for Drone Operators and Pilots, 2019, 6-7.
[26] Ways in Which the GDPR Will Impact the Drone Sector, 2018, <https://dronerules.eu/en/professional/news/5-ways-in-which-the-gdpr-will-impact-the-drone-sector> [04.09.2023].
[27] Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, October 2022, 37, <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf> [04.09.2023].
[28] Spanish Data Protection Agency, Drones and Data Protection, 2019, 3, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].
[29] 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, 2017, 14.

aforementioned article, thereby triggering the data controller's obligation to conduct an impact assessment on data protection.

It should be noted that the responsibility to conduct an impact assessment lies with the data controller. While it is possible for another individual to carry out the assessment, the data controller remains accountable for this obligation.[30]

In the process of assessing the impact on personal data protection concerning the use of drones, attention should be given to the following issues: defining the operational area of the drone; tracking the movement of processed data (which involves a systematic description of the processing procedure); establishing the necessity and proportionality of data processing; identifying potential threats and evaluating their impact; and outlining measures to mitigate or address identified risks.[31] It is crucial for drone operators to incorporate risk-based and risk management strategies into the construction and operation of drones. Before deploying a drone, operators should conduct an analysis of potential threats to personal data protection, this analysis should aim to strike a fair balance between the interests of data subjects and the drone operator.[32] Additionally, factors such as the intended operation's purpose, the type of drone to be utilized, and the technologies integrated into it should be considered during the evaluation process.[33]

It is recommended that experts and stakeholders should be involved in the impact assessment process. Additionally, it's crucial to engage the Personal Data Protection Officer (if applicable) to facilitate a thorough assessment.[34] Furthermore, whenever feasible, it's preferable for the data controller to consult with the data subjects or their representatives during the preparation of the impact assessment. For instance, when using a drone in a populated area, such communication may involve local residents, businesses, neighborhood associations, as well as educational, medical, political, or religious institutions in the vicinity.[35]

The impact assessment on data protection should be perceived as a tool that helps the data controller make informed decisions about data processing[36], which allows them to determine whether the use of a drone is truly necessary and appropriate for achieving a specific goal.[37]

3. Analysis of European Approaches

Across the European Union, regulations outlined by both the GDPR and national personal data protection laws govern the protection of personal data when using drones.

[30] Ibid.
[31] Data Protection Impact Assessment Template, Resource for Ddrone Operators and Pilots, 2019, 3.
[32] *Tarr T., Tarr J.A., Thompson M., Wilkinson D.*, Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 3.
[33] Spanish Data Protection Agency, Drones and Data Protection, 2019, 5,
<https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].
[34] 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, 2017, 15.
[35] Data Protection Impact Assessment Template, Resource for Drone Operators and Pilots, 2019, 5.
[36] 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, 2017, 14.
[37] Information Commissioner's Office (ICO), UK, Additional considerations for technologies other than CCTV, October 2022, 36.

However, in addition to these legislative acts, various specialized documents may also address personal data protection issues related to drone usage. These may include manuals prepared by supervisory bodies, internal regulations governing civil aviation, and documents developed by the European Union in this field.

3.1. Regulation (EU) 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft

In the European Union exists regulation concerning the rules and procedures for operating unmanned aircraft, which outlines specific conditions for the use of unmanned aerial systems, including the relevant personnel, remote pilots, and organizations involved in these operations.[38]

Separate articles of the regulation address personal data protection concern in the operation of unmanned aerial systems. For instance, Article 12, paragraph 2 stipulates that for an individual to receive authorization to operate a drone, they must undergo a successful assessment, which includes a declaration by the drone operator confirming compliance with EU legislation, including regulations on personal data protection. Additionally, the regulation outlines procedures for registering drone operators if the drones they operate are equipped with systems capable of processing personal data.[39]

In addition, the regulation mandates specific obligations for an unmanned aerial vehicle operator as outlined in its annex, according to which operators are required to take appropriate measures to ensure that their planned operations are in compliance with the General Data Protection Regulation (GDPR). This includes the preparation of a data protection impact assessment, which must be conducted upon request from the national data protection authority.

3.2. United Kingdom — Drone and Model Aircraft Code

In addition to personal data protection legislation, the United Kingdom has an active "Drone and Model Aircraft Code"[40], established by the Civil Aviation Authority, with one of its chapters dedicated to safeguarding individuals' right to privacy.

Along with general calls to the need for personal data protection, the code delineates specific responsibilities for drone operators. For instance, to prevent intrusive photo or video recording that egregiously infringes upon people's privacy, operators should possess knowledge about the technical capabilities of the drones they utilize. Specifically, operators should be familiar with the drone's image recording capabilities, including its zoom functionality, and whether it allows for starting and stopping filming during flight. Additionally, the code advises operators to position themselves visibly to data subjects during filming, facilitating their understanding of who is operating the drone. Moreover, the code

[38] EU Regulation 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft, 24 May, 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0947> [04.09.2023].
[39] Ibid, Art. 14.5 (a-ii.).
[40] The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Airplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25). Published: October 2019, Last updated: January 2023, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].

emphasizes the importance for data controllers to warn data subjects before capturing photos or videos, ensuring the security of captured media, and refraining from making them public without consent.

3.3. Ireland — Guidance on Data Processing Using Drones

In May 2022, the Irish Data Protection Commission released guidance on data processing using drones.[41] "The manual defines drones as a broad category of unmanned aerial vehicles remotely controlled and outfitted with technology for capturing images, videos, sound, and/or other data, which are subsequently transmitted to smart devices such as cloud storage. Drones have the potential to transform into mobile surveillance systems and process the personal data of individuals passing by, who are considered data subjects."[42]

Accordingly, the Irish supervisory authority categorizes drone operators as data controllers, except when the drone is solely for domestic or personal use and imposes specific obligations on them to prevent irreversible infringement of data subjects' rights. Additionally, it's worth noting that "the guidelines do not cover the use of drones for law enforcement purposes."[43]

According to the guidelines, "when a data controller utilizes a drone and it is not solely for personal or household use, they are obligated to demonstrate that:

- data processing was in the interest of the data subject;
- The use of the drone is necessary to achieve the intended legitimate purpose;
- that it does not have a disproportionate impact on the data subject.

In addition, it is noted that the supervisory body, depending on a number of circumstances, may require data controllers to assess the impact of data processing and develop a privacy policy document. Moreover, data controllers must take into account:

- Their actions must comply with the laws governing the operation of drones (for example, trespassing on private property);
- They must define the initial and subsequent purposes of the data processing;
- In case of an information request from the data subject, they must provide comprehensive information about the purposes of data processing, legality, and rights of the subject;
- Data processing must be based on a legal basis;
- In the process of data processing, they must consider the principle of data minimization, the possibility of depersonalization, and pseudonymization to avoid untargeted (excessive) data processing".[44]

"In the case of using a drone for household and economic purposes, the supervisory body advises drone operators to adhere to the "principle of reasonableness" when determining the scope of data processing. They should avoid filming faces and intruding into other people's private spaces."[45]

[41] The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].
[42] Personal Data Protection Service, Worldwide Practice, June/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].
[43] Ibid, 12.
[44] Ibid.
[45] Ibid.

3.4. Spain — Guidance on "Drones and Data Protection"

In May 2019, the Spanish Data Protection Agency released a guide titled "Drones and Data Protection." This guide is designed to offer drone operators further insights and recommendations concerning issues related to personal data protection.[46]

The document states that the general obligation to comply with the provisions of data protection is determined by Article 26 of the Royal Decree No. 1036/2017, on the Regulation of the Civilian Use of Aircraft by Remote Control. However, it should considered that together with the legislation regulating airspace, the conditions established by the GDPR fully apply to data processing by means of drones, regardless of whether the drone is used for professional or recreational purposes.

The guidelines delineate between two categories of data processing arising from drone usage. Firstly, instances where the drone's intended purpose inherently involves the necessity for data processing (e.g., video surveillance). Secondly, scenarios where the drone's purpose doesn't inherently entail a requisite need for data processing (e.g., infrastructure inspection, topographical measurements, etc.), although depending on circumstances, may impact individuals' rights to data protection and privacy.

The guidelines offer precise recommendations for drone operators, such as:

- To minimize data, operators should reduce the number of individuals and identifiable objects within the frame, like license plates. This objective can be accomplished by scheduling flights during periods of low human activity in a designated area;
- Additionally, to minimize data, operators should conduct video/audio recording and/or photography only during specific moments when necessary, rather than throughout the entire flight;
- Operators must utilize data protection measures integrated into the drone, such as reducing the resolution of photos to the minimum necessary to achieve the purpose of data processing, thereby making data subjects less identifiable;
- In areas where the presence of people is unavoidable, photos should be taken in a manner that prevents the identification of individuals captured in them. For instance, this can be achieved by capturing photos from a sufficient height;
- Unnecessary information related to data subjects should be avoided during storage. For instance, if the purpose of photography is to conduct a topographic survey of the coastline, there is no need to retain photos of people vacationing on the beach.

The guide also offers the following additional recommendations:

- For installation on a drone, the most suitable technologies for the intended purpose should be selected;
- Mechanisms should be implemented to ensure proper notification of data subjects;
- To create the necessary security guarantees for the protection of data subjects' rights, appropriate technical and organizational measures should be implemented. It is particularly important to avoid the risk of unauthorized data processing during the transfer of collected data;

[46] Spanish Data Protection Agency, Drones and Data Protection, 2019, <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].

- Unnecessary personal information should be promptly deleted or depersonalized after data collection;
- The operator must ensure that both the drone and themselves are as visible and identifiable as possible to the data subject.

The manual lists specific steps a data controller must take before using a drone, including:

- The operator must check if national legislation permits the use of the drone and, if required, obtain authorization from the relevant aviation authority. Failure to comply with national laws regarding drone usage could result in data processing during such flights being deemed in violation of the principle of legality outlined in the GDPR;
- Before undertaking any action that unavoidably involves data processing, it is crucial to analyze the necessity for a data protection impact assessment. This determination should consider factors such as the purpose of data processing, the type of drone being used, and the technologies employed.
- If photographs are taken for personal use, it is important not to make them public on the Internet in a form accessible to an indefinite circle of individuals (when such photographic material allows identification of persons);
- It is necessary to assess in advance the physical safety of the flight and ensure compliance with aviation legislation.

4. Conclusion

The European standards developed around data processing by drones remain essentially similar. Special emphasis is placed on obligations related to transparency, informing the data subject, ensuring data security, and practicing data minimization throughout the data processing cycle. Additionally, when developing a new product or service, it's important to consider data protection standards (Data Protection by Design and by Default) and preparation an impact assessment on data protection. Also, it's worth noting that the new law of Georgia "On Personal Data Protection," which main part is set to come into effect on March 1, 2024,[47] imposes a number of obligations, including those directed at drone operators acting as data controllers. Hence, processing personal data in the context of drone usage in compliance with the law and international standards is crucial. Doing so will significantly mitigate the heightened risk of violating the rights of data subjects, stemming from the extensive scale and unique nature of data processed through drone operations.

Bibliography:

1. Law of Georgia “On Personal Data Protection”, 5669-rs, 28/12/2011.
2. Law of Georgia “On Personal Data Protection”, 3144-XIms-Xmp, 14/06/2023.
3. Personal Data Protection Service, World Practice, June/2022, 11-12. <https://personaldata.ge/ka> [04.09.2023].

[47] Law of Georgia on “Personal Data Protection”, 3144-XIms-Xmp, 14/06/2023, Art. 90.

4. Data Protection Impact Assessment Template, Resource for Drone Operators and Pilots, 2019, 3, 5.
5. EU Regulation 2019/947 on the Rules and Procedures for the Operation of Unmanned Aircraft, 2019.
6. 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, 2017, 14-15.
7. Information Commissioner's Office (ICO), UK, Additional Considerations for Technologies other than CCTV, 2022, 36-37.
8. Spanish Data Protection Agency, Drones and Data Protection, 2019, 1, 3-5. <https://www.aepd.es/es/documento/guia-drones-en.pdf> [04.09.2023].
9. *Tarr T., Tarr J.A., Thompson M., Wilkinson D.,* Data Protection, Privacy and Drones, Clyde & Co LLP, 2022, 1, 3.
10. The GDPR (General Data Protection Regulation) and Drones, 2018, <https://aerialworx.co.uk/gdpr-and-drones/> [04.09.2023].
11. The Data Protection Commission (DPC) of Ireland, Guidance on the Use of Drones, 2022, 4-5, <https://www.dataprotection.ie/en/dpc-guidance/guidance-on-the-use-of-drones> [04.09.2023].
12. The UK Civil Aviation Authority, The Drone and Model Aircraft Code - For Flying Drones, Model Aeroplanes, Model Gliders, Model Helicopters, and other Unmanned Aircraft Systems Outdoors in the Open A1 and A3 Categories, Protecting people's privacy (Points 20 to 25), October 2019, Last updated: January 2023, Point 22, 32-33, <https://register-drones.caa.co.uk/drone-code/the_drone_code.pdf> [04.09.2023].
13. Privacy by Design Guide, Resource for Drone Operators and Pilots, 2019, 6-7.
14. Ways in Which the GDPR Will Impact the Drone Sector, 2018, <https://dronerules.eu/en/professional/news> [04.09.2023].