National Authority for Data Protection and Freedom of Information of Hungary

Opinion on Data Processing by Drones

CONTENTS

We may observe the tendency of an increased use of the so-called drones[1] in recent years, in Europe as well as in Hungary. Apart from military use, this new technology opens up a series of opportunities for the industry, agriculture and trade, primarily through the diversified and combined use of device mounted on aerial vehicles (cameras, cargo transport, heat sensors, heat scanners, GPS transmitters, Bluetooth, Wi-Fi transmitters, motion detectors, facial recognition devices and biometric scanners, etc.) With a respect to their location in space, their specific way of movement and the fact that they most often handle personal data, their use leads to issues about privacy and data protection. At present, *Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC, Annex II*, regulates the use of drones, stipulating that safety regulation of remote controlled aircraft with an operating mass exceeding 150 kg shall be laid down by the European Aviation Safety Agency in a regulation. However, flight safety rules pertaining to remote controlled aircraft weighing under 150 kg shall be laid down by Member States' Aviation Authorities. No specific legislation on drones or remote controlled aircraft has been adopted as yet in Hungary; the legislation ruling the subject in detail is now under preparation. The use of such equipment is provided for through individual permits today, and the Aviation Authority of the National Transport Authority is the competent authority to issue them.

One may expect that the use of drones will be widely adopted, primarily as they offer cost-efficient solutions for commercial use when equipped with a variety of accessories, while private users may enjoy the convenient, entertaining and efficiency-improving functions of this new technology in the future. One must also bear in mind that the use of this technology offers a series of benefits for government purposes. These typically include use for disaster management, crime prevention, law enforcement, border control, ambulance and health service purposes.

One should point out in general, that the use of drones do not pose a data protection issue per se; the problem arises with the atypical data processing through the accessories installed on drones. As compared to data processing up till now, the main difference lies in the fact that even proper use means a severe violation of people's privacy, as the device is able to collect data about anything in its field of vision, and this field of vision is unusually broad and versatile in comparison to the

[1] In line with the ICAO definition, remotely piloted aircraft including drones constitute a subgroup of the unmanned aerial vehicles. Unmanned Aerial Vehicles, also referred to as UAV are aerial vehicles that do not require a control crew on board, and which conduct the flight independently, without human operators. Remotely Piloted (Aerial) Vehicle, also known as RPV or Remotely Piloted Aircraft System, RPAS, is a set of configurable elements consisting of a remotely-piloted aircraft, its associated remote pilot station(s), the required command and control links and any other system elements as may be required, at any point during flight operation. (From: ICAO CIR328, 2011) Drones are aerial vehicles with autonomous or remote control, or often with a combination of the two, which therefore do not require a pilot on board (source: Wikipedia).

scope of similar technologies up till now. In the absence of relevant regulations, a drone cannot be tracked or avoided like a helicopter-mounted camera or a CCTV installation, and is able to follow individuals or objects in motion, without being detected. This new technology easily enables the data controller to conduct covert surveillance as the transport device providing for the observation activity (i.e. the drone) may be of the tiniest size whose detection is difficult or impossible, and may change its position quickly and unnoticed. One may see that drones' functions and characteristics largely differ from sports and model aircraft, hot air balloons and other aerial vehicles and the image recording devices that may be fastened upon them, and therefore it is right to declare that drone technology presents new quality in comparison to older technologies. In addition, management of data recorded by drones is done by a fully automated system, which makes it difficult or impossible to modify it during flight. Another significant difference lies in the fact that the amount and diversity of data recorded during flight provides for data collection that is different from the original purpose, thus enabling the new technology to go as far as creating data pools or allowing bulk data gathering. Data processing by drones is conducted mid-air. Its object may have been recorded from unusual altitudes or position up till now, and the data subject may even be unaware of being targeted. Should the data subject be able to find out about being targeted, they may still not know who to address and how to exercise their rights. We may therefore establish that the inappropriate use of this new technology enables gross violation of people's privacy, and alters the boundaries of one's private sphere primarily by being able to collect personal data from a great distance while airborne, and thus the citizens may have to be prepared for impacts against their most intimate private sphere at a scale previously unexpected. The use of drones may also impact privacy and its public image even when not recording personal data. In summary, we may establish that privacy- and data protection-related concerns arising from drone-controlled data processing are unprecedented when compared to the capabilities of other similar technologies.

The mere existence of drones may affect the right to privacy and other human rights in the following ways:

- the fear of being observed may alter the behaviour of people;
- the use of drones makes the violation of people's psychological and physical dignity easier and simpler than ever before;
- for the time being, the technology remains incomprehensible for private persons;
- there is an extremely high risk of non-compliant data processing;
- a high degree of vulnerability in the anonymity of the human body and human dignity;
- a high degree of vulnerability in the privacy of the home and private property;
- the significance of negative impacts on the right to freedom and safety, on the freedom of association and assembly, on religious freedom, on the freedom of expression and on the principle of non-discrimination;

With respect to the above and to the prospect that this entirely new technology is expected to spread widely within a short time, the Authority has drafted its opinion to offer guidance for legislators and users. This guidance looks at the data protection issues arising from the civil use of drones, while the military use remains outside the scope. The Authority reserves the right to modify these recommendations in the light of new pieces of legislation, and as the domestic and international scientific views and the public image of the new technology are changing shape.

One may look at the subject from several angles[2]. The Authority has identified three main categories of the users as government, commercial and private, and endeavours to draft its recommendations for these three areas of use, with the following objectives in mind. As government activities are largely regulated in the legislation, these recommendations hope to propose that data processing by drones should be conducted for the purposes laid down in the relevant legislation and should not be used for unlawful covert surveillance, bulk data gathering or profiling[3]. Our recommendations for commercial use[4] focuses on the enforcement of data protection and privacy when proposing an administrative permit procedure, mainly to make sure that fundamental rights affected by the technology should remain under adequate protection. Finally the Authority recommends that the scope of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as Privacy Act) be extended to the use of drones by private persons in public spaces (as an exception and only to data processing by drones).

---

[2] Drones in Canada: Will the proliferation of domestic drone use in Canada raise new concerns for privacy? Report prepared by the Research Group of the Office of the Privacy Commission of Canada (2013) https://www.priv.gc.ca/information/research-recherche/2013/drones_201303_e.pdf; In the picture: A data protection code of practice for surveillance cameras and personal information, UK Information Commissioner, (2014), http://ico.org.uk/news/latest_news/2014/~/media/documents/library/Data_Protection/Detailed_specialist_guides/cctv-code-of-practice.pdf,

European Commission: Communication from the Commission to the European Parliament and the Council, A new era for aviation, Opening the aviation marker to the civil use of remotely piloted aircraft systems in a safe and sustainable manner. Brussels, 8.4.2014. COM(2014) 207 final,

European Commission Enterprise and Industry Directorate-General, ENTR/2007/065: Study analysing the current activities in the field of UAV.

[3] *A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről*. 2013.01.30. (Recommendations of the Hungarian National Authority for Data Protection and Freedom of Information on the fundamental requirements of electronic surveillance systems at work) Available in Hungarian at http://www.naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf

[4] Including data management by drones in all sectors of the economy, i.e. industry, agriculture and commerce

1. General legal overview

The regulation on the civil use of drones is under preparation in Hungary. The Authority believes that the issue needs to be regulated as a separate item in the national legislation, which should extend to the specific stipulations regulating the protection of privacy and data concerning the use of drones. The Authority claims that reference to the Privacy Act is insufficient due to the reasons explained below, and that specific legal provisions are required.

When drafting privacy and data protection regulation for drones, the existing international (Article 8 in the European Convention of Human Rights[5], Convention 108 of the Council of Europe[6], Directive 95/46/EC of the European Parliament and of the Council[7]) and Hungarian (The Fundamental Law of Hungary[8], Privacy Act) legislation in force need to be taken into consideration. One must also consider the special character of the legal issue and some of its special characteristics, while drafting data protection regulation for drones.

When drafting regulations for drones it is useful to consider the decisions made by the European Court of Justice in joined cases Nos. C-293/12. and C-594/12, Digital Rights Ireland, and Seitlinger and others[9] (based on Directive 2004/24/EC of the European Parliament and Council[10]). One must also bear in mind that the Court took a stand for the enforcement of the highest level of protection of the fundamental rights laid down in Art. 7 (right to privacy) and Art. 8 (right to the protection of personal data) of the Charta[11]. Since drones are capable of amassing personal data during government, commercial or private use, the findings of the Court on the shortcomings of the

---

[5] European Convention of Human Rights, Council of Europe, CETS 005., 1950.

[6] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS 108., 1981.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (directive on data protection), OJ 281., 1995

[8] http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=140968

[9] ECJ C-293/12. and C-594/12. Digital Rights Ireland and Seitlinger and Others, joined cases, 8th April 2014.

[10] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (directive on data retention), OJ L 105., 2006., invalicated on 8 April 2014.

[11] EU (2012), EU Charter of Fundamental Rights, OJ C 326., 2012.

directive on data retention shall also be borne in mind when drafting regulations for data collection and for the government takeover of data collected for other purposes. The regulation must therefore include guarantees that data collection and management by drones shall be limited to a specific purpose, time, location and group of people, whether it is done for public or for private purposes. Data collection and management must remain proportionate and limited to purpose. Data processing by drones shall therefore meet the requirement that it is conducted within a specific procedure based on a valid legal basis, concerning a defined group of persons or for their benefit, and that it shall not be conducted in a pooling manner, targeting large crowds and with a general purpose. When drafting regulations for the takeover of data collected for another purpose, the legislator shall pay special attention to incorporate appropriate guarantees in the text, concerning the access to and use of such data.

Data processing done by drones may require a set of data protection safeguards that differ from the same concerning other, similar object of regulation (e.g. surveillance cameras in public spaces, regulation on the use of aerial photographs), as drones can provide for atypical data registration and management as explained earlier. Therefore, the Authority finds it insufficient to make reference to the regulation concerning other such surveillance devices (e.g. surveillance cameras in public spaces, regulation on the use of aerial photographs), as data processing by drones has a series of special features explained above, which calls for a separate set of regulations to be drafted for such data processing. The Authority finds that application of the regulation now in force through analogies is equally insufficient, as the special features listed above may not be regulated in a satisfactory manner with a reference to any of the rules now in force. Rules concerning surveillance cameras in public places are insufficient, since drones and consequently the recording device are often indiscernible, can shift positions at a high speed, in comparison to the fact that public surveillance cameras are static and the image- or video-recording device is clearly visible. Reference to the rules concerning the use of aerial photographs would not bring about a satisfactory result, since aerial photographs are taken from easily discernible (visible, audible) aircraft, registered by the authorities, while drones are not registered, small-sized, often indiscernible; all these reasons call for a separate regulation. Data protection requirements for Google Street View may no doubt offer a few guidelines for drones as well, however a transposition without modifications is not desirable, as that would also ignore the facts that the device is indiscernible, can shift positions at a high speed, and that data registration is not static, may even be streamed online, and repeated at frequent intervals. In addition, the drone can ’peek’ into areas other devices cannot, can record data from a position formerly unexpected, and can do it without being recognized by the data subject, as their noise may not be detected.

2. Recommendations for the legislator

The purpose of data processing

The Authority recommends that the legislation stipulate that data processing by drones shall be done only with a valid legal purpose, which shall also be in line with the legal basis of the data processing. This may be guaranteed through a permit procedure, which would include a privacy and data protection impact assessment as well. The Aviation Authority seems to be best suited to conduct the permit procedure, which shall assess and enforce the data protection considerations outlined in this recommendation. Our Authority may assist the Aviation Authority's functions in assessing more complex data protection issues with sector-specific recommendations and guidance. The legality of the data processing may be ascertained during the permit procedure before the competent authority issues said permit.

In the permit procedure, the applicant shall indicate the purpose, legal basis, time, place and content of the data processing, whereupon the Aviation Authority shall assess the following:

- Is the purpose of the data processing legal?
- Has the application for data processing been provided with reference to the appropriate legal basis?
- Is the data processing necessary, proportionate and in line with the purpose?
- Has the applicant fulfilled their obligation to provide information completely?
- Are the conditions of legal data processing fulfilled?

During the permit procedure the Aviation Authority shall, as a minimum, ascertain and include the following in the permit:

- name, address and contacts to the data controller;
- purpose, place, time and content of the data processing;
- the extent of personal data recorded and their retention time;
- details of fulfilled obligation to provide information;
- significant details of the data recording technology and data security system(s) involved;
- manners of deleting unnecessary personal data and making them unrecognisable, unidentifiable and inaccessible;
- name and access to the contact person assigned with the exercise of the rights of the data subject.

Scope

It might be important that the personal and area scope of the act shall extend to all data produced, collected and transferred by every drone operating in the Hungarian air space, as well as to all data pertaining to natural and legal persons and economic entities without legal personality staying in the country (irrespective of the drone's origin and destination).

Legal basis

It is of explicit importance that the law define the legal basis for processing of personal data. The Authority finds that reference to the relevant stipulations in the Privacy Act is adequate in this context.

Necessity

Personal data shall only be processed to an extent and during a period necessary to fulfil its purpose. The Authority therefore recommends that the legislator consider the principle of 'privacy by design', and draft legal stipulations attached to the individual data processing purposes to make sure that these do not exceed the requirement of necessity. As an example, if the law requires that a drone record flight data which might contain personal data, the Authority recommends to incorporate a provision in that legislation to guarantee that these personal data are to be recorded separately from the flight data and anonymously, or that the data controller render these data unrecognizable, unidentifiable and inaccessible, upon completion of the flight. Several technological solutions are available for such operations, please see Opinion 05/2014 on Anonymisation Techniques by the Data Protection Working Party established in line with Art. 29. of the Directive on Data Protection[12] for guidance, but the most important task of the legislator remains to make sure that personal data collected and managed by drones shall be used to the extend and during a period deemed necessary for the data processing purpose only.

Proportionality

Data processing by drones shall fulfil the requirement of proportionality, and similarly make sure that any personal data recorded by drones shall be managed to an extent proportionate to the data processing purpose. When regulating the aspects evaluating the data processing purposes, the legislation shall stipulate that the authority issuing the permit shall assess what may be considered as proportionate data processing. The Authority points out for the legislator that the principle of

[12] Opinion 5/2014 of the Working Party in line with Art. 29 on Anonymisation Techniques, WP 216, Brussels, 10 April, 2014.

'privacy by default' shall be realized in practice as a necessity. As a result, devices installed on drones shall be defined, configured and licensed in a way that they are unable to collect and manage an amount of data disproportionate to or different from the data processing purpose. When conducting anti-theft surveillance of an area, recording the face and movements, etc. of passers-by would constitute disproportionate data processing, which must be pointed out for the applicant during the permit procedure, and such activities shall not be permissible, in line with the Authority's view. It is even more advisable to configure and install private security device on drones in a way they cannot record faces, movement or body temperature, and can only indicate the location and fact of alleged trespassing at a certain area. This example clearly shows the significance of a privacy and data protection assessment conducted during the individual permit procedure, whereby the Authority evaluates and grants permit to the data processing operations one by one.

Purpose limitation

Stipulations on purpose-limited data processing in the regulation are another matter of guarantee. Personal data may only be managed under purpose limitation, anything diverging from that is not permissible, and it is equally forbidden to pool and manage personal data, as it is banned in general in the Privacy Act, and the Authority is recommending a specific ban in the regulation on data processing by drones. Another ban shall be necessary on using data recorded under purpose limitation for another purpose, not listed in the relevant permit by the authority. Consequently, one may not use pictures of a farming land for activities under the employer's right to control, whether it is done free of charge or for a fee, etc.

Obligation to provide information

Obligation to provide information is the most significant issue among drone-related privacy and data protection considerations. Data subjects may only make an appropriate decision about their personal data once they have received adequate information on the management of these data. When it comes to drones, the main problem lies in the data subjects being unaware of data processing, as the drones may be tiny, may fly at a high altitude, their noise almost or fully inaudible, and therefore may not be discernible. In addition, the identity of the data controller remains hidden when the drone has been observed, as the data subject will only see a tiny aerial vehicle without being able to find out about the operator, the owner or the purpose and extent of the data processing, the recording of the personal data remains unknown and no information will be provided. With these considerations in mind, the Authority recommends that the legislator prescribe a method of identification for drone operators and users, whereby data subjects can easily identify the data controller and receive answers to the questions above. As part of the permit procedure mentioned above, we also recommend that the data controller appoint a contact person to liaise with the data subjects to provide information and for the exercise the data subject's rights, without

restricting the data subject's right provided for in the Privacy Act, to protest against the data processing in any way and through the data controller's any channel of contact, The Authority will not take a position in the choice of technology (digital, projected or radio broadcast registration number, audible signal and light indicator, a public website, signs in the public area or a combination of these) for identification, however the installation of a system will be a minimum requirement, which displays the flight route in advance, in real time and ex post, and which also enables searches. The information system may be available at a website installed for this purpose, however one must make sure that data subjects without internet connection and adequate technology shall also be properly informed about data processing by drones. The data subjects shall under every circumstance be unambiguously informed in advance about the time and place of the data processing's start relating to their personal data. Any third persons, whose personal data were recorded and are managed in an identifiable manner, shall be given the opportunity to protest against the data processing. The Authority also finds it worth considering to draw up an official register of persons operating and using drones for commercial purposes. Such a register may ease the handling of data protection issues in the practice and may also contribute to an efficient settlement of flight safety and liability issues.

We must point out now that the Art. 29 Data Protection Working Party has made a number of observations in their Opinion 15/2011 on the definition of consent[13] (hereinafter referred to as 'the Opinion'), concerning the requirements of adequate information. The Data Protection Working Party has also declared that the manner of information has special importance in assessing whether it was an 'informed consent'. The manner of information shall be in line with the content, and make it understandable for the average user. The Working Party explained in the Opinion that access to and visibility of information is excessively important: information shall be forwarded directly to the data subject. Mere 'availability' somewhere is not enough. Information shall be targeted, noticeable and complete.

The Authority points out para.1, Section 4 of the Privacy Act, which says that data recording and processing shall be fair and in line with the legislation. Consequently, under adequate information provided in advance, a fair and legal data processing requires that the data controller makes information easily understandable and accessible for anyone. In addition, the data controller must make sure that the data processing information is available and accessible.

[13] Opinion 15/2011 of the Working Party described in Art. 29, on the definition of consent, WP 187, Brussels, 13 July 2011.

The following points are recommended for consideration during the administrative permit procedure:

- Information shall be structured and easily readable.

- The Privacy Act stipulates that information on the data processing shall be available for consultation for the data subjects when recording the personal data. Due to the atypical nature of data processing by drones, this information shall be available at an appropriate time, well before the data processing begins. At the present state of the information society and in addition to the above, one may expect that data controller ensures that the information is permanently available and accessible for the data subjects (for instance at a website drawn up for this purpose).

- Information on data processing shall preferably start with the data controller's contact information, the legal basis and the purpose of the data processing, as this will bolster confidence in the data controller by ensuring that the data subjects immediately find out who and why will process their data.

- Contact information shall include a mailing address (official postal address) and electronic access (e-mail address). The data controller shall select an e-mail address whose inbox is checked regularly and replies are sent out in due course.

- The information shall also contain the address to the data controller's official website as it is the easiest channel for providing address to the information on data processing, and the data subjects will easily and simply find out how their personal data are being processed.

- The information on data processing shall also contain the data controller's official telephone number. We find it necessary to add that one may only receive general information via telephone, and the data controller may accept statements from the data subjects concerning the exercise of any of their rights (e.g. information about their data) in writing only (electronically or by mail). The written statements provide that the data controller can make sure that it is actually the data subject that has contacted the controller about the exercise of their rights, and this is the channel where the exercise of such rights can be traced.

- The information on data processing shall inform about the most important issues concerning data processing: as a minimum, about personal data retention time, retention circumstances, the most important issues concerning the right of the data subjects and rights to legal remedy.

Data security

Data security is also of high importance. Apart from classic requirements, the Authority points out two consideration as being significant, i.e. the requirements of safe data connection and of separate data processing. At present, remote-controlled aircraft, especially those in private use, mainly use the network of some internet service provider, transmitting signals with Wi-Fi. The Authority is of the opinion that transferring personal data with this method is unsafe, and recommends that the stakeholders develop a method (VPN, a separate set of tariffs, coded network, fully encrypted data transfer from endpoint to endpoint), which provides for a safe transfer of personal data. The Authority points out that the legislator shall fully comply with the content of the decision brought by the European Court of Justice in joined cases Nos. C-293/12. and C-594/12, Digital Rights Ireland, and Seitlinger and others (Directive 2004/24/EC of the European Parliament and Council)[14]. The Authority adds that data stored in drones pose data security issues, therefore such a manner of data storage is only acceptable temporarily.

Separate data processing is of equal importance, the Authority maintains. Drones process personal data that were recorded for flight safety reasons (e.g. personal data recorded for flight safety reasons while approaching the target area). It is indispensable to draft strict regulation prescribing that these data be stored separately and unidentifiably (see also the section on purpose limitation above). Convenience shall never take precedence over data security requirements, and this principle shall be a requirement for manufacturers as well. The use of drones may only be permitted in case they comply with the requirements of safe data storage and processing.

Retention period

Personal data collected by drones shall only be retained until the purpose of the data processing has been fulfilled. In practice it means that the data controller is to delete all personal data collected by the drones (the transfer and use of visual images, video and measurements), once the purpose has been fulfilled. The Authority wishes to point out that an extension of the data retention time may not be permitted for any kind of use, due to such a new technology. As a general requirement, the shortest possible time should be the primary rule, with a reference to the regulations in force. For data transferred for a purpose different from the original one, the legislation shall contain a specific ruling on retention period, which stipulates that such data may only be retained in case it is not available from another source, and may only be processed for government or authorised commercial purposes, and to an extent absolutely necessary for that purpose. The legislator is reminded that the propriety of the retention period as requested in the application shall be assessed in line with the legislation in force for government procedures, and in consideration of the data

[14] ECJ joined cases C-293/12 and C-594/12, Seitlinger and others, 8 April, 2014.

processing purpose for commercial use, and an unwarranted length of retention shall be reduced to a justifiable period.

Data processing diverging from the original purpose

This technology may impact privacy in an unprecedented manner as explained above, and that it may transfer large amounts of personal data from one data controller to another when used for purposes other than those originally listed. The Authority only finds it in line with the legal basis defined by the specific purpose, and only to an extent deemed necessary. On the other hand, the Authority recommends that data processing diverging from the original purpose shall only be permitted with a reference to a possible data processing reason, and only in case the licensing Authority has previously permitted that. For the individual, specific rules, please see recommendations for the individual data processing purposes below.

The rights of the data subjects

The Authority finally recalls that the rights of the data subjects shall be enforced to the greatest possible extent. Data subjects shall have the possibility to access their data and be informed by the data controller about the nature of personal data being processed. In addition, data subjects shall be given the opportunity to rectify, delete or block such data. Enforcing these gives tremendous significance to the obligation to register and for the authority's permit procedure. Registration and the official permit procedure will clarify the identity of the data controller beyond doubt, whom the data subjects may contact to exercise their rights.

The data controller shall allow the data subject access to the recording of their personal data, in case they wish to protest against the processing of their data or request their deletion, correction or blockage. When exercising such a right, the data subject first turns to the contact person specified at registration to clarify, how they wish to exercise their rights as data subjects. In any case, an opportunity shall be provided where the data subject may personally view the recordings made and stored of their personal data, at the data controller's official premises, and make statement about the manner in which they wish to exercise their rights. The Authority recommends that the minutes of such a procedure shall be taken to avoid any further conflicts. In case the data subject requests the deletion, rectification or blockage of their personal data, the data controller shall meet this demand immediately and on the spot, which shall also be entered into the minutes. In case the personal data may not be deleted for some reason, any further processing thereof, despite the protest of the data subject, may only be considered legal if the recording is modified in a way that makes the data subject unrecognizable, unidentifiable, inaccessible, without the possibility of finding any

relationship between the recording and the data subject. The data controller and the data subject may agree on other methods as well (e.g. sending out the recording and uploading it to a password-protected website, established for this purpose), but the target of the procedure is to ease the exercise of the data subject's rights.

The data subject shall also be provided the right to object against data processing by drones. This right gives the preliminary information explained above special significance. The data controller shall consider such an objection, when it is submitted upon publication of the preliminary information, and shall modify the details of data recording and processing, and shall duly inform the objecting data subject and the public as well, about the modification. (If, for example, the owner of the property affected by the flight or its neighbour files an objection, images of the property in question may not be recorded, and the data controller shall alter the route or, if that is not possible, leave the camera in the off mode.) These possibilities shall be made available and free for everyone, and information shall be published in a way the data subjects shall have a reasonable amount of time to exercise their rights.

The Authority believes that information may only be denied in cases laid down in the Privacy Act, and the new piece of legislation shall offer a right to appeal through the court of the Authority.

Rules for private users

Allowing for the benefits of the new technology but also bearing the dangers listed above in mind, together with the fact that this area may easily become non-transparent and uncontrollable, the legislator needs to draft rules for private users as well. It may only be done with flight safety considerations (above a certain size and specification, only registered and licensed government and commercial users may fly drones) on the one hand, and with a set of constraints in the legislation on the other. It is worth considering to limit private use to an area defined by the authorities and to prescribe a simplified permit and registration procedure in order to identify the data controller and to enforce the rights of the data subjects. It is equally advisable to outline state and municipal areas where the private use of drones is permissible, and to flag the no-fly zones as well.

In addition to the above, the Authority recommends that the stipulations of the Privacy Act shall be extended for private users when the drone is used in public places as well, but only in relation to data processing by drones and only exceptionally. The Authority shall not take a position in the issue still undecided internationally, as to what constitutes private use and how this can be differentiated from other uses, however we wish to offer an equal level of protection for the exceptionally high risk posed by data processing done by drones in private use. The reason of this strictness lies in the fact that these devices are sold together with the capacity of making image-sound- and video recordings that may contain other persons' personal data, and such data may then be shared in the easiest way in ICT media and on social networks. The storage and retention of such

personal data is entirely up to the data controller, as there are no specific rules or guidance as to who these personal data are shared with and in what manner. In the absence of such regulation, one may only refer to the Civil Code when protesting against and demanding compensation for the atypical data processing explained above, affecting other persons' exclusive privacy. As the present Hungarian legislation in force provides for the use of recordings made for private purposes, as evidence in court[15], data processing by drones continues to limit the right to unperturbed privacy, which increased the Authority's determination in this recommendation, as tracking and the observation of others, and recording their data may become a decisive element in law enforcement, which the citizens obviously need to be protected against. The relevant provision in the Privacy Act needs to be extended to this form of data processing also because of the fact that there is usually no legal basis to process data in this manner, as it is pointless to consider that the data subject has given consent as long as this person is not aware of the data processing, has not discerned it and nor can they announce an objection in time. Bearing all this in mind, the Authority maintains that a legal protection more specific and targeted than the Civil Code needs to be available against those who choose to disturb or violate other people's privacy with this new technology. The most important step is to ensure that the data subject is informed in a way it enables them to act efficiently in the protection of their privacy, personal rights and personal data.

The Authority is ready to prepare a detailed recommendation about the individual issues of the relevant provisions in the Privacy Act in case its scope were to be extended.

Special issues

The application of provisions on legitimate protection and protection of property become special issues in regulating the operation and use of remote controlled aerial vehicles. The Authority is of the opinion that an unauthorised flight may qualify as trespassing, where legal redress may be obtained through an administrative channel (from the notary and/or the court). The Authority wishes to point out that one may not act against a remote-controlled aircraft arbitrarily under the pretext of trespassing, as the unauthorised use of such aircraft does not constitute a threat against the control over the property, and only violates the unperturbed use of said property, where redress is available through an administrative way. Legal redress for the unauthorised and illegal processing of personal data may be obtained from the Authority and in court. When assessing legitimate protection and situation calling for legitimate protection, the Authority points out that in line with 4/2013. Supreme Court's decision one may claim the right to legitimate protection when having suffered an illegitimate attack. Persons conducting legitimate protection do so to protect the law against injustice. The person defending himself from the peril of an unlawful attack shall be deemed acting in justifiable defence. The person defending himself justifiably is protecting the law against unlawfulness. An attack is an activity that fulfils the legal requirements of some criminal act (infringement). The objective feature of an attack is its unlawfulness. The risk and consequence of

[15] Paragraph 78, Section (1)-(4) of Act XIX of 1998 on Criminal Proceedings and Paragraph 3 Section (5) of Act III of 1952 on Civil Proceedings

guarding off an unlawful attack shall be borne by the perpetrator. Consequently, if the drone's user commits any of the criminal acts listed in Act C of 2012 on the Criminal Code (hereinafter referred to as the Criminal Code)[16] (e.g. misuse of personal data, Section 219 of the Criminal Code, the violation of private homes, Section 166 of Act II of 2012 on Infringement, Infringement Procedures and their Registration System (hereinafter referred to as Act on Infringement[17], and harassment, Section 222 in the Criminal Code) the data subject may be entitled to justifiable defence. This will be surely looked into in detail, by the courts.

3. Recommendations for government use

- Necessity: In line with the above, personal data may only be processed for government use in compliance with the rules on necessity. Data pooling and data processing for observation or for a possibility thereof, may not be permitted. It applies especially in case of data processing for criminal purposes, where the same rule shall apply: data processing by drones shall only be used for individual cases, once the criminal proceeding has started, and in line with the rules on criminal proceedings for covert or secret observation, i.e. with a prior judicial authorisation. The Authority points out that public surveillance done by drones, bulk collection of personal data from persons or their groups do not meet the basic requirements of the necessary data processing.

- Proportionality: Processing of data recorded by drones poses the problem of proportionality, when compared to the purpose. The technology makes the collection of personal data easier than before, one must bear in mind that these data may only be processed if it is done in proportion to the purpose and if it does not exceed that measure of proportionality. Data processing for government purposes must comply with the requirements of necessity and proportionality, and one must always consider whether the purpose to be fulfilled with the use of drones may otherwise be met in a way that affects the privacy to a smaller extent. Consequently, in criminal investigations and law enforcement activities one shall always assess the activities' impact on the privacy of innocent (not suspected) persons, and select the method with the smallest impact.

- Purpose limitation: The principles laid down in Section 4 of the Privacy Act shall be observed throughout the entire data processing, and as a minimum, one must make sure that personal data may not be processed in a way different from the purpose. In other words, the

[16] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV&celpara=#xcelparam. In English: http://thb.kormany.hu/download/7/ec/a0000/14_Act%20C%20of%202012%20on%20the%20Criminal%20Code.pdf

[17] http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200002.TV

Privacy Act only allows data processing if it complies with the data processing purpose. For example, when recording measurements and images of a flood, the recordings taken on the way to and back may not be processed, similarly as the data pertaining to the neighbouring properties or people appearing in the vicinity. Data processing for government purposes shall also be limited to purpose and necessity; for instance data processing for the protection of historic sites may not include the data of its visitors, people walking by, working in the vicinity or vehicles passing by or any other characteristics. Personal data related to this purpose shall only be processed until the purpose has been completed, i.e. the controller of the aerial images may store until the completion of the flood relief and for the historic sites until restoration is finished. The recordings shall not be processed for other purposes (e.g. creation of databases, providing evidence for insurance contingencies), they may not be handed over to other persons and shall be deleted upon completion of the purpose.

- Data processing diverging from the original purpose: We need a special chapter on drone-processed data taken over by government authorities and their use for a purpose different from the original one. As we have explained above how seriously this technology violates people's privacy and how difficult it is to trace the route of the data processing, the Authority recommends that special stipulations be drafted to regulate the transfer of such recordings. These should include a definition of the legal bases that provide for the transfer of such personal data in individual cases. We recommend that such images and personal data shall only be transferred, seized and used as evidence in official proceedings in individual cases, once criminal proceedings have been launched and with a judicial warrant. The Authority is of the opinion that it is not fair to use illegally recorded evidence to as evidence in criminal proceedings or to enforce a claim under private law.

- Summary: the following points shall be considered when analysing the above criteria for data processed by drones:

    - Is the drone used legitimately?
    - Is the drone necessary to achieve the defined purpose (necessity)? In other words, is the drone indispensable to complete a given task of the government, to satisfy the need that has thus arisen, or is it just a barely cost-efficient alternative?
    - Is the purpose to pool data, to process pooled data or to conduct observation?
    - Is data processing by drones in line with the purpose? (purpose limitation) Is it exceeding the purpose?
    - Is the drone use in proportion with the purpose (proportionality)? Is there an alternative with a smaller impact on privacy? Is the impact on privacy in proportion with the expected benefits? If the benefits are relatively smaller,

e.g. resulting in a minimal saving only, the impact on privacy is not in proportion with the purpose to be achieved.

- Is there an alternative way of achieving the purpose, with a smaller impact on privacy? If alternative measures offer the same level of efficiency, the system operator shall use one of these alternatives.
- Is the chosen method efficient enough for the purpose (efficiency)?
- During data processing one must make sure that the data are accurate, complete, and up-to-date if so needed, and that the data subjects may only be identified as long as it is necessary for the purpose.
- Have the data subjects been informed? If not, was it legal to refrain from the notification?

- Obligation to provide information: Government uses shall also fully comply with the requirements to provide information listed above. Any refusal or divergence shall only be permissible exceptionally, in the cases defined in the legislation. Restriction of the right to information on grounds of public interest is only permissible in individual cases as defined in the legislation.
- Retention period: The legislation now in force shall apply, extending the retention period shall not be permissible.
- Rights of the data subject: All government bodies shall respect the right to obtain information. Rights of the data subject may only be limited in the exceptions listed in Section 19 of the Privacy Act.

4. Recommendations for commercial use

- Purpose limitation: Drones shall only be used for the purpose listed in the legislation and permitted by the authority, and to the extent and period defined in the permit. Any data processing diverging from this shall require a new permit. When defining the purpose, one shall consider the legal bases and a purpose in line with those shall be selected.

- Necessity: Only personal data required for the purpose may be recorded. Procedures and methods for deleting unnecessary personal data or making them unrecognizable, unidentifiable or inaccessible shall be provided for and listed in the application. One must bear in mind that data processing by drones may disturb people's privacy only to an absolutely necessary and unavoidable extent. Protection of personal data shall be considered throughout the entire procedure, and the Authority recommends that the data controllers develop their procedures within the framework of the future legislation in a way it has the smallest possible impact on people's privacy. The Authority points out that the principles of

'privacy by design' and 'privacy by default' as explained above, shall be adhered to. If a full record of the flight data and flight route is required for official reasons, one must provide for a recording device on the drone, which records the required data making sure that personal data shall not be legible or available, primarily by processing the recorded data in a separate and closed way, and blurring out the personal data contained therein. One must also make sure that the data shall be deleted from the drone in the shortest possible time. Navigating and recording devices shall be configured so as to record data listed in the purpose only and nothing else.

- Proportionality: Data processing by drones for commercial purposes shall be just as proportionate: the amount and extent of personal data recorded shall not exceed what is absolutely necessary for the purpose of the data processing. Special data require special treatment. Data processing for security purposes of a religious event for example shall not record the names, faces, gender or faith of the participants, as it would infringe upon the requirement of proportionate data processing. Assessment shall be made whether data processing can be conducted in a way with a smaller impact on privacy.

- Data processing diverging from the original purpose: Privacy and data protection shall be considered when conducting commercial data processing for a purpose that diverges from the original. Therefore, data recorded for a definite purpose may only be used for another purpose in case it is provided for by a legal basis defined in the legislation, and which is also included in the official permit. Consequently it is important to ensure that the principle of privacy by design shall apply in the regulation as well as in practice, and that technology shall have solutions that satisfy data protection requirements. For example, configurations shall ensure that a drone, when used to measure radiation, shall approach the target without the help of any recording device and only record data about the radiation in question.

- Obligation to provide information: The data controller shall make a special effort to provide information. As a general rule, information about data processing shall be provided at a time in advance of the data processing that allows for the data subjects to express their objection, and shall address those that are affected or may be affected by the data processing. In addition, real-time information about the data processing shall also be provided to the data subject, who will also be given the opportunity to find out about the details of the data processing and exercise their rights as data subjects, within a reasonable time after the data processing. The manner and extent of information shall always have to be customized to the given situation. Web-based information may suffice in one case and will be insufficient in another.

- Retention period: Retention period shall be specified in the permit procedure, and the personal data shall be finally and irreversibly deleted upon its expiry.

- Rights of the data subject: Data subjects shall be provided the opportunity to exercise their rights, and the data controller shall appoint a contact person that is able to receive and process the data subjects' claims and motions. A system needs to be developed, through which the data subject can find out about the data pertaining to them, in possession of the data controller, at the data controller's premises, as a minimum. One shall prepare in advance to make undeletable data unrecognizable and unidentifiable, and also to demonstrate how and where the data, blocked upon the data subject's request, shall be stored without infringing upon the rules pertaining to purpose-limited data processing.

5. Advice for private users

In lack of a domestic regulation and considering the fact that drones are available to all at a relatively low price and that private use may pose a high risk of infringement upon other people's privacy, the Authority wishes to make the following points. The recommendations below apply to certain important issues of data processing by drones, based on the legislation now in force.

- Inappropriate use of drones may easily constitute a crime or infringement (Section 219 of the Criminal Code, Section 166 of the Act on Infringement, Section 222 of the Criminal Code), where the drone is the tool of the infringement, and liability falls upon its user or operator.
- For data processing by drones the provisions of the Privacy Act shall apply until the relevant legislation is adopted.
- Subjects of data processing by drones shall be informed in a way it enables them to act efficiently in the protection of their personal rights and personal data.
- Drones may record large amounts of data of third persons and may largely infringe upon the privacy of third persons. These data and privacy shall be protected in line with the stipulations of the Privacy Act and this recommendation.
- Drones may not be used to observe and track others (unless a prior written consent has been obtained from the data subject).
- Recordings that violate other people's dignity may not be taken by drones, not even for private use.
- Special attention shall be paid to the protection of the personal data of minors, even when using drones.
- Drones may not be used for activities that are part of the authorities' competency (e.g. public safety, law enforcement, catastrophe relief, firefighting, etc).
- When using drones for private purposes, the data controller shall fully comply with the obligation of identification, where special attention shall be paid to the following points:

- Prior to use, the appropriate official permits shall be obtained, and drones shall be used for the purpose and to the extent specified in those permits.
- Data subjects shall be given the opportunity to exercise their rights. If for example images taken during a holiday contain other persons, who express their objection, use of the drone shall be suspended or limited to a group of subjects who have given consent thereto.

- The use of drones in public areas require an official permit.
- Personal data shall not be published (on the open internet and in social media) without a prior consent from the data subject.