ARTICLE 29 DATA PROTECTION WORKING PARTY

01673/15/EN
WP 231

Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones

Adopted on 16 June 2015

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION:

Executive Summary

In light of the progressive integration of drones into the European civil airspace and the emergence of numerous applications of drones (ranging from leisure, services, photography, logistics, surveillance of infrastructures) there is a real need to focus on the challenges that a large-scale deployment of drone and sensor technology could bring about for individuals' privacy and civil and political liberties and to assess the measures necessary to ensure the respect for fundamental rights and data protection.

Indeed, several privacy risks may arise in relation to the processing of data (such as images, sound and geolocation relating to an identified or identifiable natural person) carried out by the equipment on-board a drone. Such risks can range from a lack of transparency of the types of processing due to the difficulty of being able to view drones from the ground to, in any event, a difficulty to know which data processing equipment are on-board, for what purposes personal data are being collected and by whom. Furthermore, the dexterity of drones and the possibility to interconnect multiple drones further facilitates their ability to achieve unique vantage points, for example avoiding obstacles or not to be constrained by barriers, walls or fences, so to easily enable the collection of a wide variety of information even without the need for a direct line of sight, for long periods of time and across large area without intermission (with a high risk of bulk data gathering and possible unlawful multipurpose uses).

Even higher risks for the rights and freedoms of individuals arise when the processing of personal data by means of drones is carried out for law enforcement purposes.

In order to properly address those concerns, after having clarified the scope of the Opinion in light of the exemptions provided for in the Directive 95/46/EC (household exemption, processing for journalistic purposes and for law enforcement purposes), the opinion provides guidelines in order to correctly address the data protection rules in the context of drones.

Verifying the need for a specific authorisation from Civil Aviation Authorities (CAAs) when national law allows to operate a drone, finding the most suitable criteria for legitimate processing, complying with the purpose limitation, data minimisation and proportionality principles (by choosing the most proportionate technology and measures to avoid the collection of unnecessary personal data) and fulfiling, in the most appropriate manner for the case in hand, the transparency principle (by informing data subjects of the processing carried out) are obligations that should be met before operating a drone. Similarly, it is necessary to adopt all the suitable security measures and delete or anonymise that personal data which is not strictly necessary.

Besides, the Article 29 Working Party (WP29) recommends adopting the measures of privacy by design and privacy by default and suggests the data protection impact assessment as a suitable tool to assess the impact of the application of drone technology on the right to privacy and data protection. Furthermore, in order to raise awareness among users a specific recommendation is proposed to manufacturers of drones to provide sufficient information within the packaging (for examples within the operating instructions) relating to the potential intrusiveness of these technologies and, where possible, of maps clearly identifying where their use is allowed...

Among others, the opinion also addresses recommendations to European and national policy makers for the strengthening of a framework that guarantees the respect for all fundamental rights at stake, not only data protection, by also introducing specific rules ensuring a responsible use of drones (which must necessarily include respect for private areas). Furthermore, WP29 calls on policy makers for the introduction of data protection aspects among the key features of national provisions regulating the commercial use of drones (in connection with pilot qualification and

training, among airworthiness and certification requirements, while issuing/revoking operating licenses and aerial work permits), calling for a strict cooperation between Data Protection Authorities and CAAs.

WP29 also recommends manufacturers and operators to embed privacy friendly design choices and privacy friendly defaults as part of a privacy by design approach and to involve a Data Protection Officer (where available) in the design and implementation of policies related to the use of drones and to promote the adoption of Codes of conduct that can help the various industry stakeholders and operators to prevent infringements and to enhance the social acceptability of drones. Specific recommendations for the use of personal data collected by means of drones for law enforcement purposes are also set out. In particular, law enforcement data processing carried out by means of drones should, as a rule, not allow for constant tracking and technical and sensing equipment used must be in line with the purpose of the processing.

1. Introduction

With a view to enabling the progressive integration of Remotely Piloted Aircraft Systems (RPAS)[1] into civil airspace[2], the European Commission adopted the Communication COM(2014)207 "*A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*" which responds to the call of the European manufacturing and service industry to remove barriers to the introduction of drones for civil use in the European single market[3].

The opening up of the drone market would require the introduction of an adequate regulatory framework by the adoption of, where necessary, national policies and common European standards, to be developed by European Aviation Safety Agency (EASA). The Article 29 Working Party (WP29) notes, in that respect, the lack of an adequate regulatory framework in most member States. In this context, the harmonisation and the modernisation of Member States' aviation polices in relation to drones should be encouraged.

WP29 acknowledges the social and economic benefits of the civil use of drones, and its potential on growth and jobs but it considers it equally important to highlight to all the threats and risks to data protection and privacy resulting from a large-scale deployment of drone technology and to assess the measures necessary to ensure the respect for all other fundamental rights at stake[4].

Indeed, the processing of personal data by drones has a peculiar nature due to the unique vantage point that magnifies the effectiveness of any on-board sensors and implies a reduced transparency and increased privacy intrusion compared to a similar fixed sensor in spite of their perceived similarities - consider, for example, video surveillance by drone versus the use of a fixed CCTV camera.

The integration of drones into the European aviation market and their different civil purposes (including the use for law enforcement) will pose specific challenges which must be overcome in order to "*respect the rights and principles enshrined in the Charter for Fundamental Rights of the EU, and in particular the right to private life and family life (Article 7) and the protection of personal data (Article 8)*"[5] and, in this perspective, the involvement of lawmakers in the debate relating to the integration of drones into the civil airspace will be indispensable.

Balancing all the rights and interests at stake will be a challenge that cannot be ignored by policy makers in order to guarantee that Europe can be at the forefront in this new sector whilst not

---

[1] Remotely Piloted Aircraft Systems is a subcategory of unmanned aircraft, commonly known as drones. It is defined by ICAO, Unmanned Aircraft Systems (UAS), Order Number: CIR328, 2011, Glossary as "an aircraft where the flying pilot is not on board the aircraft". For the sake of simplicity, the term "drone" will be used throughout this opinion as an encompassing term to refer to those systems.

[2] See European Council, Conclusions: 19/20 December 2013, Euco 217/13.

[3] It should be recalled that a similar process is underway in the USA. For an up-to-date overview of the different steps taken by the Federal Aviation Administration in this field see https://www.faa.gov/uas/.

[4] Such as human dignity, right to liberty and security, freedom of thought, conscience and religion, the freedom of expression and information, the freedom of assembly and of association, and the right to non-discrimination.

[5] European Commission Services, Staff Working Document "*Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)*", SWD(2012)259 final, 4 September 2012, p. 21. For a recognition of the need of a "broad assessment of privacy threats" associated to the use of drones, see also the European RPAS Steering Group, "Roadmap for the safe integration of civil RPAS into the European aviation system", 20 June 2013 and its Annex 3 "A Study on the Societal Impact", p. 28. The privacy aspects of drone applications were taken into considerations also in the recent Opinion on the Ethics of Security and Surveillance Technologies presented to the European Commission by the European Group on Ethics in Science and Technology on 20 May 2014.

forgetting that "*the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity [and] on the principles of democracy and the rule of law*"[6].

This Opinion responds to the call made by the European Commission[7] with a view to providing practical indications to legislators and regulators (at both the European and national level, including Civil Aviation Authorities (CAAs[8]), industry, policy officers and the public at large. This includes addressing the impact on privacy and data protection and the consequences of the extended use of different drone applications for all various civil uses. Peculiarities and criticalities related to compliance with specific requirements under the existing data protection legal framework are considered. The Opinion concludes with recommendations on how to adequately address risks that may arise in connection with drones and the purposes of their use in order to make the processing of personal data lawful and compliant with the data protection legal framework.

2. Description of the phenomenon and of the impact on privacy and data protection

2.1 Definition, features and potentialities of drones

According to the International Civil Aviation Organisation (ICAO), a Remotely Piloted Aircraft System (referred to here as a drone) 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*"[9].

Generally speaking, drones are aerial vehicles that can belong to different categories with a wide variety in specification, features and capability[10]. Drones can be designed to support a variety of payloads ranging in size and technical capability. The most basic type of drone consisting only of vital components[11] may not be processing personal data but can still cause annoyance and social disturbance to others. Adding other sensors for other purposes such as to record audio or video data raise obvious data protection and privacy concerns. It is however important to recall that commercially available drones are not necessarily equipped with on-board cameras or other sensors by default and it may be the choice of the drone operator to include such a capability, depending on the type of use. A drone can also be designed and built by the operator himself sourcing components from a range of suppliers.

Some examples of equipment that could have an impact on privacy and data protection are:

- Visual recording equipment: Smart cameras with fixed or variable focal length, capable to store and transmit live images, with on-board or ground-based facial recognition capabilities, allowing drones to identify and track specific individuals, objects or situations, identify patterns of movement, to read license plates on vehicles, whilst guaranteeing a 360° view, enabled to detect

---

[6] Charter of Fundamental Rights of The European Union, Preamble.

[7] On 6 May 2014, the European Commission's DG Enterprise and Industry addressed a letter to the WP29 inviting the DPAs to issue "*recommendations on how to address the privacy and data protection issues at European level and what actions should be undertaken to underpin the establishment of an adequate framework*".

[8] Safety regulation of large RPAS (> 150 Kg) is the competence of the EASA, while regulation of light RPAS (<150 Kg) is the competence of national CAAs (see Article 4(4) and ANNEX II of the Regulation (EC) No 216/2008).

[9] ICAO, Unmanned Aircraft Systems (UAS), Order Number: CIR328, 2011, Glossary.

[10] Their dimensions can vary from a few centimeters to several meters, and their flight envelopes can be very different too, including slow flight and hovering capabilities like many rotorcrafts, or high-speed and high-altitude operations like high performance aircraft. The control of drones by remote pilots is usually based on multiple data links and command links provided by radio equipment or by data links established through the Internet via digital wireless access links, with remote pilots working on the ground (or onboard of another vehicle), in many cases within the line of sight. For operations beyond line of sight a navigation system, relying on positioning systems like GPS, and telemetry equipment is strictly required for the pilot's situational awareness during the flight, sometimes enriched by live images from onboard cameras.

[11] E.g. frame, motors, rotors, battery, receiver and flight controller.

the thermal energy emitted by a target, allowing the flight and the recording of images in poor visibility conditions (due to fog, smoke, or debris) or during night hours;

- Detection equipment: optical-electronic sensors, infrared scanners, synthetic aperture radars to identify objects, vehicles and vessels and obtain information on their position and course even behind walls, smoke, or other obstacles;
- Radio-frequency equipment: such as antennas capturing the location of Wi-Fi access points or cellular stations, femtocells and IMSI catcher used by law enforcement agencies to control cellular phones and networks or by service provider to relay communications among networks and terminal users;
- Specific sensors for the detection of nuclear traces, biological traces, chemical material, explosive devices.

Besides, the extent to which drones can be modified and adapted to specific situations and their relative low cost is resulting in drones being applied to a range of novel scenarios[12]. However, in any case, it has to be made clear that the relevant point, from a privacy and data protection standpoint, is not the use of drone per-se but the data processing equipment on-board the drone and the subsequent processing of personal data that may take place. Indeed, it is the processing of images (including images of individuals, houses, vehicles, driving license plates, etc.), sound, geolocation data or any other electromagnetic signals related to an identified or identifiable natural person carried out by the data processing equipment on-board a drone that may have an impact on privacy and data protection and therefore trigger the application of data protection legislation[13].

2.2 Data protection risks

In the light of all the existing applications and others in the foreseeable future, several risks have already been highlighted in terms of safety, third party liability and privacy[14]. Indeed, as for this last aspect, it is likely, in a number of cases, that data subjects would not be aware of the drone or any processing of their personal data which is being carried out given that these devices can be difficult to view from the ground. In any event, even if individuals are aware that a drone is in the area it is difficult to know which data processing equipment are on-board, for what purposes they are being collected and by whom. This will result in an increased feeling of being under surveillance and a subsequent possible decrease in the legitimate exercise of civil liberties and rights, best known as "chilling effect"[15].

---

[12] Their deployment in "3D" operations – i.e. dull, dirty or dangerous – is extremely attractive from a health and safety perspective given that the human operator can remain some distance from the hazardous location. So drones can be used in the traditional areas of aerial work represented by surveillance, reconnaissance, search and rescue, environment monitoring, agriculture, and also in other areas related to entertainment and sports, journalism and news, documentary, logistics and transportation, construction and public works, network and infrastructure monitoring and maintenance and for law enforcement purposes.

[13] See, in this regard, the definition of "personal data" and "data processing" set out in Articles 2(a) and 2(b) of the Directive 95/46/EC. It should be highlighted that data collection without any recording or storage is nevertheless a processing operation that entails the application of the data protection legislation and that "*identifiability within the meaning of the Directive may also result from matching the data with information held by third parties, or else from the application, in the individual case, of specific techniques and/or devices*" (Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, WP89, p. 15). For an extensive guidance on the interpretation of the notion of personal data, see Article 29 Data Protection Working Party, Opinion 04/2007 on the concept of personal data, WP136.

[14] Among others, see the abovementioned "A Study on the Societal Impact" Annex to the "Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System", passim.

[15] On the chilling and panopticon effect syndrome arising from a large-scale use of drones, see Rachel L. Finn, David Wright and Anna Donovan (Trilateral Research & Consulting, LLP), Laura Jacques and Paul De Hert (Vrije Universiteit Brussel), *"Privacy, data protection and ethical risks in civil RPAS operations*", 7 November 2014, at http://ec.europa.eu/DocsRoom/documents/7662, p. 28 et seq. and elsewhere.

The dexterity of drones further facilitates their ability to achieve unique vantage points, for example to avoid obstacles and to not be constrained by barriers, walls or fences. Drones can therefore more easily enter private premises, so to easily enable the collection of a wide variety of information from a variety of sources. Depending on the technologies on-board, data could be collected without the need for a direct line of sight (i.e. through roofs, debris or clouds), for long periods of time and across large area without intermission (with a high risk of bulk data gathering and possible unlawful multipurpose uses).

One should also consider the possibility of interconnecting a number of drones in order to carry out surveillance on a large area. Swarms of drones, with real-time communication channels between them and external parties, trigger yet higher data protection risks, since they could easily enable coordinated surveillance, i.e. tracking movements of individuals or vehicles over large areas.

Thus, there is a high risk that the processing of personal data by drones becomes covert and causes a major interference with the most intimate sphere of individuals. At the same time, there is an undeniably higher risk of function creep (i.e. the risks of changes or extension of use for incompatible purposes), considering the potentially sophisticated equipment on-board and the ease with which the collected personal data can be linked with other pieces of information.

Besides, the potential impact of the privacy intrusion is compounded by the wide constellation of stakeholders and entities involved in their use. Manufacturers of drones, for example, have also a role to play in the design phase of drones as the operational features may, to a greater or lesser extent, lend themselves to privacy-intrusive applications (e.g. in the case of small or micro-sized drones capable to fly inside buildings).

The perception of drones by individuals is inextricably linked to their social sustainability. In this respect, the effective application of data protection law may contribute to the acceptance of drones. Therefore, WP29 encourages the initiatives and awareness raising projects that accompany the introduction of drones on the EU civil market.

3. Legal analysis

Although there is no specific legislation on the data protection implications of the use of drones in Member States, the relevant legal framework is made up by the Data Protection Directive 95/46/EC (hereinafter the Directive) and, as far as drones may also be used by providers of publicly available electronic communications services (e.g. for extending the reach of such services), Directive 2002/58/EC, as amended by 2009/136/EC.

Furthermore, in spite of the different impacts that the use of drones can have on the privacy and freedom of individuals, in comparison with CCTV systems, there might be circumstances where national legal provisions applicable to CCTV systems may also apply to the use of drones, in particular in case of drones used for video surveillance purposes. In the light of this, WP29 would like to refer to its Opinion on the processing of personal data by means of Video Surveillance stressing the topicality of the legal analysis and the recommendations provided therein[16].

Nevertheless, due to the abovementioned peculiarities and risks of drone applications, WP29 deems it important to give specific guidance on how to comply with data protection rules in this context.

This being the framework, great attention should be given to the issue of data controllership especially considering the wide gamut of drones-based services already offered by specialised companies to public and private organisations. In the light of that, it is of the utmost importance that

[16] Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, id.

controller and processor should be clearly identified for each type of drone operation especially by evaluating the essential elements to distinguish the controller from other actors[17]. Clear guidance for identifying the different combinations of responsibilities among different entities involved in joint processing may be found in the WP29 Opinion 1/2010 on the concepts of "controller" and "processor"[18].

3.1 Applicability of the Data Protection Directive

While the European Commission is focusing its attention on remotely piloted aerial drones, this Opinion does not differentiate between fully autonomous and non-autonomous unmanned aircraft systems, considering that this aspect is not relevant vis-à-vis the data protection issues arising from the use of this kind of technology. Furthermore, the guidelines should apply – with the necessary adjustments – to data processing arising from the use of any kind of aerial vehicle (manned or unmanned, aeronautical or spatial) for civil operations.

However, it should be highlighted that some instances of processing of personal data deriving from the use of drones for civil operations may fall out of scope of these guidelines in the light of exemptions or derogations that, according to the Directive, Member States can lay down (see, in particular, Articles 3, 9 and 13).

Pursuant to Article 3.2 of the Directive, the processing of personal data by a natural person in the course of a purely personal or household activity will be out of the scope of this Opinion.

Nevertheless, the provision set forth in Article 3.2 is an exception and, as such, it must be narrowly construed. Hence, as considered by the European Court of Justice, the so called "household exemption" must "*be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*"[19]. Furthermore, if the operations of a drone and the equipment on-board are such as to give raise to a video surveillance system, to the extent it involves the constant recording and storage of personal data and covers, "*even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46* "[20].

Moreover, according to Article 9 of the Data Protection Directive, Member States could provide for exemptions or derogations from some of its provisions[21] in case of processing of personal data

---

[17] A controller "determines the purposes and the means of the processing of personal data" (Article 2 d) of the Directive). A processor shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (Article 2 e) of the Directive). For instance, while this role could be clear when the drone is used directly by a company who bought it for delivering packages (controller), a different framework could be envisaged in case a company commits mapping of an area to a drone operator (in this case the company is the controller and the operator is the processor).

[18] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP169.

[19] European Court of Justice, Judgment in Case C-101/01, *Bodil Lindqvist case*, 6th November 2003, para 47.

[20] European Court of Justice, Judgment in Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33. See later in this paper for the requirements that this application will entail in terms of lawfulness, proportionality, transparency, security measures, etc., considering that, as recalled by the European Court of Justice, "*the application of Directive 95/46 makes it possible, where appropriate, to take into account — in accordance, in particular, with Articles 7(f), 11(2), and 13(1)(d) and (g) of that directive — legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself*".

[21] In particular, those relating to the general rules on the lawfulness of the processing, the rules on transfers to third countries and the rules on supervisory authority and WP29 (Articles 6 (1), 10, 11 (1), 12 and 21 of the Directive).

carried out solely for journalistic purposes or the purpose of artistic or literary expression[22]. Nevertheless, the exemptions and derogations should only be those "*necessary to reconcile the right to privacy with the rules governing freedom of expression*".

The processing of personal data carried out by means of drones for journalistic reasons should therefore take into account the different national laws and provisions applying to this kind of processing. However, Member States should be aware of the potential intrusiveness of these instruments, especially if used in an irresponsible and unethical way, and should clearly identify the duties and responsibilities carried with the exercise of freedom of expression by the aid of drones.

WP29 attaches the utmost importance to the introduction of an appropriate framework at national level (if this is not already in place) so that the use of drones for strictly personal and recreational purposes and for journalistic purposes[23] does not impinge on fundamental rights to privacy or confidentiality of communications and that the respect of a reasonable expectation of protection of private life even in case of collection of personal data carried out in public places could be ensured. As recalled by the European Court of Human Rights, there is a "*zone of interaction of a person with others, even in a public context, which may fall within the scope of private life*"[24]. Therefore, general principles and some specific suggestions laid down in this Opinion should be also taken into account by legislators and regulators (both at national and European level) when laying down the requirements to be complied with for the use of model aircraft[25] and by the public in general in order to avoid breaching the data protection legislation and other pieces of national legislation safeguarding other personal rights[26].

3.2 Processing of personal data for law enforcement purposes

Drones may signal a fundamental transformation of law enforcement practices, in particular regarding the role of data in guiding law enforcement actions, ranging from monitoring an individual to determining targets from a review of the lives and activities of a specific population

---

[22] An activity could be classified as a journalistic one as far as its "object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit-making purposes" (European Court of Justice, Judgement on the Case C-73/07, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, 16 December 2008, para. 61). Similarly, the European Court of Human Rights considered that "the function of the press includes the creation of forums for public debate. However, the realisation of this function is not limited to the media or professional journalists" (see European Court of Human Rights, Judgment on Case Társaság a Szabadságjogokért v Hungary, 14 April 2009, para. 27).

[23] In this regard, for example, the adoption of code of conduct for journalistic purposes could be advisable in order to address this issue taking into account all different interests at stake.

[24] European Court of Human Rights, *Judgment on Case of Von Hannover v. Germany (n. 2)*, 7 February 2012, para. 95. See, in this line, European Data Protection Supervisor, Opinion on the Communication "*A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*", 26 November 2014, page 7. By carefully balancing the different interests at stake, Member States – which are all States Parties of the ECHR – would also fulfill the positive obligation to ensure the effective respect for private and family life that derives from Article 8 of the Convention (see European Court of Human Rights, *Judgment on Case Airey v. Ireland*, 9 October 1979, para. 32, *Judgment on Case Marckx*, 13 June 1979, para. 31).

[25] The abovementioned ICAO Circular 328 (point 2.4) recalls that model aircrafts fall outside the provisions of the Chicago Convention, but could be the subject of relevant national regulations. In this framework, the introduction of specific rules ensuring a responsible use of drones could be envisaged, which must necessarily include respect for private areas (such as gardens, courtyards, terraces, etc.) and for a "reasonable expectation" to privacy even in public areas; to that end, the introduction, when needed, of virtual perimeters might be envisaged. In this regard, see, for example, the Italian Regulation on Remotely Piloted Aerial Vehicles (Article 23).

[26] The distribution of leaflet to be packaged together with the model aircraft, for example, could be useful in order to call attention to the necessary respect of data protection principle, where applicable, and other pieces of national laws. An interesting example of leaflets for the personal use of drones ("*Règles d'un bon usage d'un drone de loisir*") could be found at http://www.developpement-durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf. See also, in that respect, the list of Do's and Don'ts for flying model aircraft issued in US by the FAA published at http://www.faa.gov/uas/publications/model_aircraft_operators.

based on continuous surveillance. Thus, the use of drones directly operated by the police and other law enforcement authorities – or their request to access data collected by drones operated by private entities for their own purposes – creates high risks for the rights and freedoms of individuals and directly interferes with the rights to respect for private life and to the protection of personal data protected under Article 8 of the European Convention of Human Rights ("ECHR") and Article 7 and 8 of the European Charter of Fundamental Rights ("Charter").

Therefore, following Article 52(1) of the Charter and Article 8 (2) ECHR, this limitation to the exercise of the rights and freedoms recognised by the Charter must be provided for by law ("in accordance with the law"), made only if it is necessary and genuinely meets objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others ("in pursuit of one of the legitimate aims set out in Article 8 (2) of the ECHR and necessary in a democratic society") .

As a result, the police and other law enforcement authorities using drones should make sure they have a valid legal basis for processing personal data.

Drones shall only be used where a concrete demonstration of their necessity and appropriateness for the specific purposes pursued is offered. In this regard, WP29 draws attention to its Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector.

The aforementioned authorities shall justify why instruments existing at their disposal and why less intrusive alternatives would not achieve such purpose (and a prior evaluation by the Data Protection Authorities may be applicable and could be envisaged for this purpose where national practices favour such prior evaluation).

In addition, when law enforcement authorities process data collected by drones for enforcement of civil offences, they should comply with requirements laid down by the Directive. In particular, such uses of drones should be restricted to cases where the processing is necessary in order to protect the vital interests of the data subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

Once and if the necessity of drones for police or law enforcement purposes is established, following Article 52(1) of the Charter and Article 8 of the ECHR, their use should comply with the principle of proportionality and specific data protection requirements: it should go no further than needed to fulfil the legitimate aim being pursued.

In this perspective, the principles laid down in the Convention n. 108 of the Council of Europe and the Recommendation No. R (87) 15 regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987 should be followed as well as the relevant principles of the Framework Decision on Data Protection 977/2008.

Besides, WP29 recalls that data processing by drones by governmental services should be conducted for the purposes laid down in the relevant legislation and should not be used for indiscriminate surveillance, bulk data processing, data pooling and profiling: limits must be imposed on the use of drones for surveillance activities, with the aim of avoiding them from becoming pervasive or being used for signalling targets based on data analysis. Therefore, drones should only be used in strictly enumerated and justified purposes that could be listed in advance and, in any case, the use should be geographically confined and time-limited. With a view to the "chilling effect" the use of drones can have on the rights to freedom of expression and freedom of assembly, particular attention should be paid to the need to protect, as far as possible, public demonstrations and similar gatherings from any kind of surveillance.

3.3 Lawfulness of the processing and purpose limitation principle

In order to be lawful, the processing of personal data entailed by the civil application of drone technology should be based on one of the criteria for making data processing legitimate that are set forth in Article 7 of the Directive[27]. Recalling the opinion on legitimate interest that provides extensive guidance on this aspect[28] and taking into account the peculiarities of the processing of personal data carried out by means of equipment on-board drones, different legal bases could be considered as relevant according to the different purposes of the processing at stake:

- freely given, specific and informed consent (Art. 7a)
  While consent is a common legal basis to be relied upon, it seems that in this context it could be considered appropriate only in few cases, especially as far as data are collected in public areas. Consent should indeed be freely given, specific and informed. In most of the cases at issue, it would be very difficult to meet all these requirements since the consent, for example, would not be "freely given" whenever an individual is not free to enter or leave a surveyed area without being under surveillance; consent will not be "informed" if that individual is not provided with all the necessary information on the processing, nor will it be "specific" if it is not possible for the individual to identify each purpose of the processing he/she is requested to consent to[29].
  Consent could be an appropriate legal basis for the processing of personal data carried out by means of a camera on-board a drone for instance in the case of a training session of a sports team (i.e. with no spectators present).
- processing necessary for the performance of a contract to which the data subject is a party (Art. 7b)
  The processing of personal data is lawful on the basis of Article 7b of the Directive, for example, when someone purchases a product that is delivered to his domicile by the seller via a drone, or when video recording services only relating to data subjects' properties are proposed by companies operating drones; however, it should be considered that incidental processing of data of non-affected third parties is never covered by the fulfilment of obligations for the parties to a contract and therefore, in the above examples, the collection of personal data of third parties should be avoided or a different legal basis should be found to legitimise it.
- processing is necessary for compliance with a legal obligation or necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed (Art. 7c and 7e)
  These legal bases could be relied on in cases in which a legal obligation imposed by law is to be fulfilled by the controller, such as the surveillance of an archaeological site required by a specific provision or, for example, in some "security-related uses", such as smuggling control, only where the use of drones is strictly necessary and proportionate.
- processing is necessary in order to protect the vital interests of the data subject (Art. 7d)
  This legal basis could be relevant in some cases of "safety-related uses" of a drone such as disaster relief, fire scene inspection, rescue of victims of snow and mountain accidents, etc. However, considering that 7(d) is meant to be strictly interpreted, a better approach may be to

[27] However, in all cases in which the usage of drones could entail the processing of special categories of data, Article 8 of the Directive will apply.

[28] See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller, WP217, page 16 et seq.

[29] See Article 29 Data Protection Working Party, *Opinion 15/2011 on Consent*, WP187.

consider these uses under Article 7(c), 7(e) or 7(f), depending on the circumstances of the case[30].

- processing is necessary for the purposes of a legitimate interest (Art. 7f)
  Personal data may also be processed if this is necessary for the purposes of the legitimate interests pursued by the controller or by the third party except where such interests are overridden by the data subject's interests or fundamental rights and freedoms (it is foreseeable that such a criteria could be envisaged, for example, in case of drone operation necessary for pipe or power line inspection or for critical infrastructure surveillance or aerial photogrammetry, atmosphere and meteorological research, wind energy monitoring, hurricane tracking, archaeological site mapping, sea ice monitoring, wildlife research)[31], if appropriate safeguards are implemented in the system.

Besides and with a look at one of the abovementioned risks triggered by the collection of a vast amount of data by drone applications and so-called "function creep", it should be recalled that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Article 6.1.b of the Directive)[32].

Therefore, any further processing of personal data for a different purpose from the one for which they have been collected should be made in accordance with the provisions of the Directive and therefore should have an autonomous legal basis and its compatibility with the original purpose should also be assessed on a case-by-case basis[33].

Furthermore, in accordance with the lawfulness principle (Article 6.1.a of the Directive), any drone operation that involves the processing of personal data should, first of all, comply with applicable law in general[34], including national regulations on CCTV and on the use of drones[35].

3.4 Proportionality, data quality and data minimisation principles: the relevant role of privacy by design and by default

As personal data may only be processed if adequate, relevant, and not excessive in relation to the purposes for which they are collected, a strict assessment of the necessity and proportionality of the processed data should take place (Article 6 of the Directive). Personal data shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data.

---

[30] See also Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller*, WP217, page 20 and 21.

[31] Useful guidance could be found with regard to this legal basis in the WP29 Opinion on legitimate interest. Ibid. However, in the light of the potential seriousness of the interference with data protection and privacy of other persons triggered by the use of drones, according to the judgment of the European Court of Justice in the Google Spain case, it is clear that such processing will hardly be justified by merely the economic interest which the controller has in that processing (European Court of Justice, Judgment in Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González*, 13 May 2014, para 81).

[32] So, for example, it should not be possible to further use images of agricultural lands, captured when ensuring that pesticides are rightly disseminated, in order to record data on neighbouring lands and techniques or to film an area to secure it and use the images/videos to fine people who did not pay for the entrance.

[33] See Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, WP203. Another significant example of incompatible use of personal data see Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, Wp128, p. 15. Furthermore, the respect of the purpose limitation principle is, for example, of key importance in case of mutualisation (see above, paragraph 2.1).

[34] Data protection legislation plus other applicable law, including national legislation safeguarding personal rights, image, family life and the private sphere.

[35] For these reasons, in Members States where the operation of drones violates national aviation rules, the processing of personal data collected during the operations will be deemed not to be compliant with the lawfulness principle.

Moreover, the data minimisation principle could be respected by choosing the proportionate technology and by adopting measures of data protection and privacy by default, i.e. privacy settings on services and products which should by default avoid the collection and/or the further processing of unnecessary personal data[36]. A less intrusive payload should be always preferred and, whenever appropriate, for example, the implementation of anonymisation techniques – as laid down in the Opinion 05/2014 on Anonymisation Techniques[37] – could be envisaged whenever processing of personal data is unnecessary.

Furthermore, in relation to the various technologies that are able to electronically read and process biometric data (facial recognition, behavioural identification), an updated analysis and useful clarifications and recommendations can be found in WP29's Opinion on developments in biometric technologies[38]. For example, when using drones equipped with video cameras, technical arrangements could be used by controllers to automatically process the images by using blurring or other graphical effects, in order to avoid the collection of images of identifiable persons whenever they are not necessary.

The application of data protection by default measures entails that, beforehand, the principle of data protection by design is respected by manufacturers and operators. Data protection should be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal; such technology should be engineered in such a way as to avoid the processing of unnecessary personal data (for example, in case of strategic or critical infrastructures, engineering firmware of drones in order to inhibit data collection within previously defined no-fly zones could be advisable)[39].

Given the variety of drone applications, in order to assess their impact on the rights and freedom of persons and in particular on the right to privacy and data protection, a data protection impact assessment could be carried out. It helps operators to discover the privacy risks (if any) associated with the use of new applications and to evaluate whether the processing of personal data via drones is legitimate, necessary and proportionate to the purpose, while covering, among others, transparency issues and security aspects and documenting the steps taken to address those risks[40].

In the light of that, WP29 would call on competent policy makers, both at European and/or national level, to evaluate the opportunity, while dealing with the new legal framework for the integration of drones into civil European airspace, to foster the implementation, as a good practice, of a data protection impact assessment for each type of drones operation which may involve the processing

---

[36] For instance, if data is stored onboard a device it should be removed as soon as reasonably practicable and retained by the data controller in a safe and secure manner in line with clearly defined retention policies. The long-term storage of collected data on a device is put at unnecessary risk from loss of theft on a later flying mission. On the other hand, drones deployed for delivery of a package are unlikely required to be equipped with cameras enabling face recognition or audio recording capabilities. A device used to monitor a roof for storm damage should not be required to record footage from the entire flight, especially if this location of interest is some distance from the take-off and landing location. In this respect, involving a Data Protection Officer (where available) in the design and implementation of policies related to the use of drones could be advisable.

[37] See Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, WP216.

[38] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, WP193.

[39] Mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and that data are especially not collected or retained beyond the minimum necessary for those purposes are envisaged by the European Commission's Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11 final (see, in that regard Article 23).

[40] In this context, first of all, for each type of drone application, a prior evaluation should take into account the types of necessary/standard data that could be collected. For example, the simple collection of data relating to the drone flight (such as altitude, airspeed, length of the flight) may not immediately trigger the application of the data protection obligations, unless the pilot or other individual are identifiable from the data (e.g. the pilot's name or employee number is included within the log meta data).

of personal data in the light of the foreseeable risks arising from the intended applications, by also providing stakeholders (manufactures and operators) with an easy-to-use set of criteria.

In particular, as data protection rules should be respected insofar as personal data are processed, a privacy and data protection impact assessment should be envisaged for manufacturers in cases of drones "designed and produced" for surveillance purposes and for operators using drones carrying on-board any kind of "audio-visual" equipment, taking into account – as said before – the payloads and the purposes of the collection and the further processing of personal data[41].

In cases where drones have an image recognition system, implementation of a mechanism facilitating exercise of the data subject's objection in the form of active or passive tags which would clearly communicate the data subjects' intentions in the face of processing of their image or devices used by them as currently used visual tags the aim of which is to show the photographers at public conferences how the image of photographed persons can be used should be considered[42].

3.5 Transparency and information to data subjects

According to the principle of fair processing (Article 6(a) of the Directive), data subjects must be aware of the collection and processing of their personal data and therefore they should be informed in line with Article 10 of the Directive, subject to the exemptions provided for in Articles 11 and 13. As soon as reasonably practicable and if a disclosure to a third party is envisaged, at the latest when the data are first disclosed, in accordance with Article 11 of Directive, data subjects should be given the following information: the identity of the controller of the drone and of his representative, the purposes of the processing for which the data are intended, any further information, such as the categories of data, recipients or categories of recipients of the data, the existence of the right of access to and the right to specify and correct the data concerning them.

To meet this requirement for transparency and information to data subjects, data controllers should consider a multi-channel approach[43]. The customary arrangements such as signposts or information sheets for an event (e.g. with a race entry pack of a rowing race) or in the event literature (e.g. sports programme) could be easily used for drone operations in fixed locations (on the occasion of sport events, concerts, in archaeological areas, natural parks, etc.) and may rely on symbols for ease of recognition and concise form. Social media, public display areas in confined locations (e.g. TV screens at a sports stadium), emitted wireless signal, flashing lights, buzzers and bright colours could also be envisaged. Moreover, ensuring that the drone operator is highly visible facilitates the exercise of other persons' rights. The requirement to display a registration mark (similar to a vehicle license plate) is only relevant in so far as drones are visible from ground level or if there is a loss of control and stored data have to be linked back to the operator. Requiring the transmission of a wireless registration mark signal which can be cross referenced with an online database is another

[41] The performance of a data protection impact assessment is envisaged in specific cases by the abovementioned European Commission's Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (see, in particular, art. 33).

[42] The mechanism of using tags signalling the data subjects' consent to the use and publication of their image was described in the Offlinetags project (see: http://offlinetags.net/en).

[43] Indeed, the WP29 acknowledges that the use of RPAS raises a challenge on how to provide information and to trigger the data subject to consult information about a device which is sometimes so invisible that he or she will not notice its presence or the collection of data. Even if informing the data subject attending an open-air event is easily conceivable through privacy notice panels located at the entrance of the RPAS-monitored zone, the question arises as to how to provide information on RPAS that will fly over the public space, without clear territorial scope limitations.

interesting solution. However the data protection and data security concerns which are raised by a registration system must also be borne in mind[44].

Additionally, as good practice, WP29 recommends that drone operators publish information on their website or on dedicated platforms in order to inform constantly about the different operations that have taken place and on forthcoming ones while, in remote areas or where it is unlikely that individuals will access the website, information can be published in newspapers, leaflets or posters, or given by letter in a mailbox[45].

In some member states, the CAA publishes the list of operators allowed to make a professional use of drones and/or of the authorisation granted for each operation. Such kind of lists should be welcomed since they may facilitate the access to information regarding data processing operations. Furthermore, since in many member states where the use of drones is regulated, for different reasons, operating drones is not allowed in some areas, the publication of maps (realised by CAAs that manufacturers can indicate, for example, by publishing a link to a info resource managed by CAAs) showing the areas where drones can be used would be very useful (i.e. the publication of this map would help people identify the areas in which drones may be operating).

The same multichannel approach could be advisable in cases in which drones are used to carry out surveillance on large infrastructure (for example, railway networks or electrical grids). The information may be given by signposts and symbols and, where possible, websites. Such information could be given in a general nature explaining that the infrastructure is being monitored – no details on forthcoming or past flights, for example, are necessary.

Finally, as for drone applications that may cover larger areas, where the provision of information to data subjects proves difficult or quite impossible, the creation of a national or cross-national information resource (easier to be found than websites of single operators) to enable individuals to identify the missions and operators associated with individual drones has been suggested[46]. WP29 acknowledges the desirability of such a solution and calls on the European Commission to make use of funding instruments to support researches and investments on this aspect, on possible smart license plates for drones and similar.[47]

3.6 Security of data processing and related issues, storage periods, prior checking

In accordance with Article 17 of the Directive, data controllers and processors, where applicable, must implement appropriate technical and organisational measures to protect personal data processing from accidental or unlawful destruction or accidental loss, alteration, unauthorised

---

[44] For example, if a pharmacy makes regular delivers by drone to an individual's property it may be inferred that the occupant suffers from a severe medical problem. Requiring an individual to submit drone flight plans or providing the ability to query the historical flights of an individual drone user or organisation, including take-off and landing sites, is likely to raise significant data protection concerns.

[45] For example, an estate agent, using a drone to record footage of a property for sale, could write to neighbors in advance but also visit the nearby properties on the day of recording alerting them to the processing.

[46] Working Group on Data Protection in Telecommunication, *Working paper on Privacy and Aerial Surveillance*, 54th meeting, Berlin, September 2013, published at www.berlin-privacy-group.org

[47] In certain high sensitivity contexts, one might also envisage the introduction of feedback mechanisms which verify the accomplishment of specific data protection related steps. As for specific actions envisaged under Horizon 2020 and COSME to support the development of the RPAS market, see European Commission, *Communication "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner"*, ibid., Action 6. The task of maintaining this resource (which could be a dedicated website where drones could be tracked in advance, on time, afterwards, and/or a publicly accessible central register) could be entrusted, for instance, to the EASA or to the national aviation authorities or to the DPAs and an obligation to report to them could be also introduced by lawmakers – not only as for the planned flights, but also regarding the purpose of the processing of personal data that will take place. In this regard, it should be recalled that anyway, in most cases, CAAs need to be informed about any drone activity in order to give authorisation. See, in this regard, para. 3.8 of the present Opinion.

disclosure or access. This provision also applies to electronic and cyber-attacks (i.e. remotely tampering with the device to either take complete or partial control over it or gain access to the sensors or the stored data).

This protection should also be provided for the transmission phase of personal data from the drone to the base station. It is recommended that designers of drones and equipment tailored to be assembled to the drone engage with appropriate security experts to ensure that security vulnerabilities are properly addressed.

Furthermore, personal data processed via drones cannot be stored for a period longer than necessary for the purpose of the processing[48]. Those data which are not linked to any complaint or issue should be deleted or anonymised immediately thereafter.

The incorporation of storage and deletion schedules could be advisable. Hence, the devices carried by drones should be designed in such a way as to allow the setting of a defined storage period of personal data collected and, as a result, the regular automatic deletion of personal data which is no longer necessary in accordance with deletion schedules.

In connection with all these aspects, WP29 would like to draw attention of data controllers, at least, to the following:

- A limited number of authorised persons, to be specified, should be allowed to view or access the recorded images
- Limited access should be granted to the abovementioned persons, on a need-to-know basis
- Encrypted storage and transmission of information where necessary
- Logs of all instances of access to and use of recorded material
- Stringent data storage periods and automatic deletion or anonymisation once the data storage period has expired
- Data breach notification to the DPA (as far as legally mandatory)

According to the relevant national data protection laws, additional measures and arrangements might result from the preliminary assessment of the processing in accordance with the prior checking mechanism (see Article 20 of the Directive).

4. Role of the cooperation between different actors and the importance of self-regulatory tools

An important role in raising awareness among manufacturers, operators and pilots on the data protection issues linked to the use of drones mounted with sensors equipment will be played by the cooperation between DPAs and CAAs. Training courses, public events, common leaflets could be used to address this topic. Furthermore it should also be considered whether there are stages within the existing processing carried out by CAAs for licensing drones pilots and certifying drones operators which might offer a good opportunity to address privacy or data protection aspects related to the use of drones.

In most cases, certifications or very specific authorisations are granted by CAAs which regulate the use of civil drones: the flight area and path, the device and the operator and controller are all often examined in this context[49]. In some countries, compliance with data protection requirements is

[48] For example, the images/videos captured by drones with the purpose to secure the open-air area of a festival shall only be retained for the time necessary to investigate possible complaints or security related issues.

[49] See, on this aspect, the results of a research conducted among the CAAs published in Rachel L. Finn, David Wright and Anna Donovan (Trilateral Research & Consulting, LLP), Laura Jacques and Paul De Hert (Vrije Universiteit Brussel), "*Privacy, data protection and ethical risks in civil RPAS operations*", page 145 et seq. and, for a description of the existing European and National drones regulation framework, page 363 et seq.

already part of a discretionary examination that is carried out by the competent aeronautical authorities when granting permissions to operate aircrafts[50]. This being the framework, informing the competent CAA of having taken into account all the requirements set forth by the data protection legislation, of the envisaged processing of personal data and of their purposes is a good practice to be supported since it could also help in calling the attention of the operators on the aspects related to data protection before any authorised flight[51] and might help realise a publicly available central database in which, at least, a list of operators (including a generic description of the purposes they might process personal data for) could be kept[52]. This is not to say that CAAs will take on the responsibility for checking that the drone operator has taken appropriate steps to comply with national data protection legislation but it is a useful checkpoint that will force the drone operator to make a conscious decision regarding the steps that they will take and whether they regard these as sufficient.

The promotion of Codes of conduct and/or certification schemes for manufacturers and operators could be envisaged in order to improve civil drone operators' awareness and understanding of data protection issues as well as with a view to help DPAs monitor compliance. The important role that Codes of conduct might have in this framework is even more conceivable considering that DPAs cannot assess or pursue broader privacy infringements where those fall beyond their legal powers, whilst this is where the accountability of drone operators can come in useful.

Finally, a helpful role could be played also by privacy seals. Even though such schemes shall not excuse data controllers from knowledge of their data protection and privacy commitments, the participation of drone operators and manufacturers in a general privacy seal approach could be supported as a means towards accountability and compliance.

5. Final indications and recommendations

In light of the potential risks and consequences that the opening of the aviation market to drones would entail for individuals' privacy and civil and political liberties, WP29 would call to the attention of European and national legislators, manufacturers of drones and relevant equipment, and drone operators/users the following indications and recommendations, which are intended to provide guidance that is additional to the one already contained in WP29 opinions and documents that are referred to in the present Opinion.

5.1 Steps to be taken before operating a drone:

1. Check if the national law allows operating drones and verify the need for a specific authorization from the CAAs;
2. Clarify the roles of possible different actors: as far as the processing is not carried out directly by the controller, ensure that the processing is governed by a contract or legal act binding the processor to the controller and that the processor acts only on instructions from the controller;

---

[50] Ibid. For example, the licence examination to be taken by a RPAS pilot might include some background knowledge on privacy and data protection legislation, to make sure that the pilots are aware of the legal obligations in case of processing of personal data.

[51] For example, in Germany the air traffic regulations (Luftverkehrs-Ordnung (LuftVO)) were amended in 2012 to include compliance with data protection requirements as part of a relevant discretionary examination by the competent aeronautical authorities of the Federal States when granting permissions to operate aircraft.

Similarly, the Regulation on Remotely Piloted Aerial Vehicles adopted in Italy on 16th December 2013 provides that "where the operations carried out by a RPAS could lead to the processing of personal data, this fact must be referred to in the documentation submitted for the granting of the relevant authorisation" (Article 22).

[52] This may also address security concerns, since recent news showed that drones were illegally flying over strategic buildings of urban areas without any possibility to identify the persons operating the drones.

3. Evaluate the data protection impact taking into account the purpose of the operations and the type of drones (dimension, visibility, etc.) and the specific combinations of sensing technology on-board it; identify the most suitable legal basis (consent of the data subjects, performance of a contract, legal obligation, legitimate interest, etc.) and the possible need to notify/consult the competent DPAs according to national data protection law;
4. Choose the most proportionate technology on-board and adopt all suitable measures of privacy by default: set services and products in such a way as to avoid the collection and/or the further processing of unnecessary personal data;
5. Find the most appropriate way to give advance notice to those who can be impacted by the data processing: inform through signposts or information sheets in case of visual operation in a specified area; in case of an event, inform public by means of social media, newspapers, leaflets or posters; give clear information always on the relevant website: the information notice should contain a clear indication of the controller and the purposes of the processing and should give data subjects clear and specific indications for exercising the right to access visual and non-visual records concerning them;
6. Take all the appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, in particular, to prevent any unauthorised processing also during the "transmission" phase;
7. Delete or anonymise any unnecessary personal data soon after the collection or as soon as possible.

5.2 Recommendations to policy makers and sector regulators

The opening of the aviation market to the civil use of drones should go hand in hand with:

1. The promotion, at European and national level, of a framework in order to guarantee not only flight safety but also the respect for all fundamental rights. In this perspective, WP29 calls for an involvement of relevant stakeholders in the debate relating to the integration of drones into the civil airspace;
2. The harmonisation and the modernisation of Member States' policies relevant in relation to drones, including the issue of the law applicable to cross-border drones operations;
3. The introduction, as part of the above framework, of specific rules ensuring a responsible use of drones, which must necessarily include respect for private areas (such as gardens, courtyards, terraces, etc.); to that end, the introduction, when needed, of virtual perimeters – or no-fly zones – might be envisaged. In addition, since the use of drones can be limited to very specific areas in many Member States, the publication of maps by the CAA would help users understand where the use of drones is permitted (given that the other principles are respected);
4. The introduction of an obligation, at European and/or national level, for manufacturers to only market small drones jointly packaged with sufficient information (for examples within the operating instructions) relating to the potential intrusiveness of these technologies and recalling the need to respect European and national legislation and regulations protecting privacy, personal data and other fundamental rights;
5. The development and introduction by the competent policy makers, at European and/or national level, in close consultation with industry representatives, of data protection impact assessment criteria that industry and operators can easily use;
6. The introduction of data protection aspects among the key features of national provisions regulating the commercial use of drones (in connection with pilot qualification and training, among airworthiness and certification requirements, while issuing/revoking operating licences and aerial work permits, etc.); in particular, declarations of having taken into

account the data protection requirements could be part of the conditions under which a permission will be granted;
7. The promotion of data protection certifications in order to improve civil drones operators' awareness and understanding of data protection issues as well as with a view to monitoring compliance;
8. Furthermore, WP29 recommends that the European Commission makes use of funding programmes to support researches and investments for new technologies intended to increase transparency (new technologies for informing the public at large of flying drones and their purposes and exercising their rights of access) including, for example, smart licence plates or website that would publish information in real-time about all drone operations.

5.3 Recommendations to manufacturers and/or operators

1. Embed privacy friendly design choices and privacy friendly defaults as part of a privacy by design approach;
2. Involve a Data Protection Officer (where available) in the design and implementation of policies related to the use of drones;
3. Promote and adopt Codes of conduct that can help the industry and different categories of operators prevent infringements and enhance the social acceptability of drones; such Codes should contain sanctions in case the signatories do not comply with the code;
4. Make the drone as far as possible visible and identifiable (using emitted wireless signal, flashing lights or buzzers, bright colours);
5. When in line of sight, make the operator clearly visible and identifiable with signage as the individual responsible for the drone;
6. When planning and operating a flight, even where allowed to operate the drone over populated areas, avoid as far as possible to fly over or near private areas and buildings.

5.4 Recommendations for the use of personal data collected by means of drones for law enforcement purposes

Similarly to the use of drones for commercial purposes, the use of personal data collected by means of drones by the police and other law enforcement authorities should:

1. Comply with the necessity, proportionality, purpose limitation, data minimisation and privacy by design principles; a strict and justified retention period should be set;
2. The transparency principle should be respected: the data processing carried out by the use of drones should be laid down/prescribed by law to be transparent and foreseeable to data subjects; as far as possible, the latter should be informed of the processing and their corresponding rights;
3. Law enforcement data processing carried out by means of drones should not allow for constant tracking of individuals or, at the very least, where constant tracking is found to be strictly necessary, this should be restricted to law enforcement warranted investigations. Technical and sensing equipment used must be in line with the purpose of the processing;
4. The prohibition of automated enforcement of decisions also applies to these uses. The data processed via drones should be further scrutinised by a human operator before any decision adversely affecting an individual is made;
5. Courts should generally be able to review the use of drones for intelligence and law enforcement purposes in line with national practice;
6. A regular review of the necessity to process personal data by the use of drones and of compliance of this use with evolving legal frameworks shall be carried out;

7. In addition, the use of drones for law enforcement, even in case of warranted investigations – such as targeted surveillance –, should require a sufficient higher regime of approval in the organisational hierarchy. Depending on national law, personal data collected by the use of drones for these types of investigations must be incorporated in the administrative files that may be used in court.