Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner"

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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,[1]

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Article 28 (2) thereof,[2]

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008[3] on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

I.1 Consultation of the EDPS

1. On 8 April 2014, the Commission adopted a Communication to the European Parliament and the Council on 'A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner' (hereinafter "the Communication")[4].

[1] OJ L281, 23.11.1995, p. 31.
[2] OJ L8, 12.1.2001, p. 1.
[3] OJ L350, 30.12.2008, p. 60.
[4] COM(2014) 207 final, 8.4.2014.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

2. RPAS are aircraft systems piloted from a distance or, in other words, aircrafts that can fly without requiring an onboard pilot. Most of the time, they are not used as a simple aircraft system, and include devices such as cameras, microphones, sensors, GPS, which may allow the processing of personal data.

3. As will be further developed in this Opinion, the rights to private and family life and to data protection, as guaranteed in Article 8 of the Council of Europe Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the EU, apply to this emerging technology. Moreover, since remotely piloted aircraft systems have the same potential to seriously interfere with the rights to private and family life and to data protection as the online technologies considered by the Court of Justice of the European Union in the *Digital Rights Ireland*[5] and *Google Spain v AEPD*[6] rulings, they must be considered very carefully.

4. The EDPS therefore welcomes the fact that we have been consulted by the Commission on this Communication.

I.2. Background and objectives of the Communication

5. The Communication's objective is to open the aviation market to the use of remotely piloted aircraft systems (hereinafter "RPAS" or "drones") to civil uses, as opposed to military uses. The Communication therefore identifies the most common possible civil uses, such as infrastructure monitoring and photography or even transport of goods and people, and insists on the importance of enabling the introduction of commercial RPAS on the EU market while safeguarding the public interest.

6. While the Communication underlines the social and economic benefits of the civil use of RPAS in the EU, in particular as regards jobs and growth, it also notes the absence of an adequate regulatory framework in most Member States. It therefore highlights the need for harmonisation of Member States' aviation safety policies in relation to RPAS and identifies technological developments that will be required to operate RPAS safely. It addresses the issues of third party liability and insurance and identifies privacy, data protection and security as key elements with which to ensure compliance for the dissemination of RPAS. Furthermore, it announces the EU support for market development and European industries.

7. The EDPS notes the choice made by the Commission to refer to *Remotely Piloted Aircraft Systems*[7] *(hereinafter "RPAS")*, to designate what is commonly known as *drones*. We also note that the Communication focuses on RPAS which are a sub-

[5] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*, judgment of the Court (Grand Chamber) of 8 April 2014 (requests for a preliminary ruling from the High Court of Ireland (Ireland) and the Verfassungsgerichtshof (Austria))

[6] Case C-131/12., *Google Spain SL, Google Inc.v Agencia Española de Protección de Datos (AEPD),* judgment of the Court of 13 May 2014.

[7] RPAS is the term used by the International Civil Aviation Organisation (ICAO).

category of *unmanned aircraft systems* ("UAS")[8] and does not clarify why UAS are not covered.

8. Since the Communication focuses on the opening of the aviation market to the *civil* use of RPAS, it should be highlighted that the word "*civil*", in this context, covers all areas not covered by military uses of RPAS, i.e. :

   - uses by companies, public authorities and professionals to monitor large-scale infrastructures such as bridges, plants, nuclear plants, railways, apply pesticides on agricultural land, inspect electricity networks, carry out aerial mapping, monitor a concert zone, secure an area, deliver pizzas or books orders, take wedding pictures, or report on an event;

   - law enforcement uses which may be, for instance, search and rescue, disaster response, border control/protection, civil protection, aerial surveillance, traffic monitoring, observation and pursuit of criminal suspects, or observation of civil unrest;

   - other "*non-military*" uses which may also include uses by intelligence agencies, some of which may fall outside the scope of EU law;

   - private uses by citizens as a hobby[9] (such as model aircrafts activities, photography, information technology).

9. However, this list should not be perceived as comprehensive since, as implied by the Communication, the nature and extent of potential RPAS operations are difficult to predict at this stage[10].

I.3. Aim of the EDPS Opinion

10. Whenever personal data is processed by RPAS operated in the EU, the EU legal framework for data protection applies in principle.[11] Together with other requirements (including aviation safety rules, certification/type-approval, health etc.), the respect of data protection requirements and the right to private and family life will enhance the development of the market of RPAS within the EU in compliance with the fundamental rights of the individuals concerned. In fact, only those RPAS that will have integrated data protection and privacy in their design will be well regarded by society at large, that is, not only by data protection

[8] According to the definitions given by the International Civil Aviation Organization in the Cir 328/190 (available at http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf), an unmanned aircraft system (UAS) is an aircraft and its associated elements which are operated with no pilot on board whereas a Remotely-piloted aircraft is an aircraft where the flying pilot is not on board the aircraft. This is a subcategory of unmanned aircraft. A remotely-piloted aircraft system 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] This might include aerial filming but also "IT enthusiast" experiments with different kinds of sensors attached to the RPAS.

[10] See Communication page 3, part 1 "RPAS can offer a myriad of new services".

[11] In this respect, we note that transnational operations carried out by RPAs may give rise to questions of applicable law. See also in this respect para 40.

authorities, not-for-profit fundamental rights organisations and associations but also by the public at large.

11. The EDPS therefore welcomes that the Communication not only underlines the expected social and economic benefits but also identifies privacy, data protection and security as key elements with which to ensure compliance for the dissemination of RPAS[12]. Their added value to activities such as agriculture, journalism or infrastructure monitoring is obvious but it is crucial to ensure that, whenever they imply the processing of personal data, their use complies with data protection law. As stated in the Commission's Communication, compliance with data protection requirements will preclude that their capacities[13] "represent a threat to citizens' privacy"[14].

12. This Opinion identifies several situations where RPAS process personal data and where controllers are, therefore, subject to the existing applicable data protection framework. It responds to the consultation of the EDPS on the Communication and aims at ensuring that further legislation on the subject takes data protection fully into account. It also aims at raising awareness of the public at large (manufacturers, controllers and data subjects) in this regard.

13. This Opinion does not aim at analysing all the data protection requirements that should be met for operating RPAS. This may be the subject of guidance by the national data protection authorities, by the Article 29 Working Party or even by the EDPS in its supervisory role if RPAS were to be used by EU institutions and bodies to process personal data.

II. GENERAL COMMENTS

II.1. In most of their uses, RPAS process personal data

14. As such, RPAS are aircraft systems, which do not *per se* process personal data. However, as stated in the Communication[15], once combined with other technologies, they offer many applications, and therefore give rise to very diverse, commercial, professional, law enforcement, intelligence, and private uses.

15. Most of the time, these technologies enable or imply the processing of personal data and therefore trigger the application of the data protection framework. For instance, many RPAS that will be introduced on the market will include a video camera device with specialised software to process the video feed. This camera device with its specialised software may well have capabilities such as high power zoom, facial recognition, behaviour profiling, movement detection, or number plate recognition.[16] RPAS could also be equipped with Wi-Fi sensors, microphones

[12] See Communication page 7, part 3.4 on the Protection of citizens' fundamental rights.
[13] Their mobility (speed and changes of altitude) and general capabilities (endurance, quiet flights and sensors mentioned previously).
[14] See Communication page 4.
[15] See page 1, title 1.
[16] In due course, possibly to be complemented by thermal sensors, night vision, synthetic aperture radar, see-through imaging (ceilings/walls),and mixed with algorithms and in the future artificial intelligence.

and audio recording systems, biometric sensors processing biometric data, GPS systems processing the location of the person filmed, or systems reading IP addresses of all devices located in a building over which the RPAS will fly. Embedded technologies could also include the possibility to track devices carrying RFID chips and persons/vehicles wearing them.

16. The embedded technology will thus offer the possibility to collect, record, organise, store, use, combine data allowing operators to identify persons directly or indirectly[17]. This identification could be done by a human operator, by automatically screening the image taken against the facial recognition programme of an existing database, by scanning to detect a smartphone and use it to identify the person, by using RFID in passports, etc. As a result, RPAS can be used to process personal data, in the meaning of Article 2(a) of Directive 95/46/EC[18].

II.2. RPAS enable processing of more personal data than planes and CCTV

17. The EDPS takes the view that RPAS should, firstly, be distinguished from manned flight systems since the capacities embedded can reveal far more than the naked eye. RPAS can be used with technology that improve on human vision, and capture details that humans cannot see. In addition, their "mobility and discretion" enable them to be used in many more circumstances than manned flight systems.

18. Secondly, RPAS equipped with video cameras obviously share many common points with CCTV systems. They allow for continuous recording or triggering of the recording based, for instance, on movement detection. However, their mobility and discretion offers more and also increasingly different uses. In other words, they give the most sophisticated cameras wings. For instance, RPAS allow imagery to be captured that would not be available if the camera were terrestrially bound (private properties with high fences, high level terraces, garden). Besides, contrary to cameras which are visible most of the time, RPAS are not always visible from ground level. Both their mobility and discretion make it easier to track individuals. The need to mask parts of the zones filmed in order to respect individuals' privacy raises more challenges due to constant mobility and zoom possibilities.

19. Moreover, when combined with other technologies, RPAS may become extremely powerful surveillance tools. Because they can carry a multitude of sensors, perform systematic surveillance (overt and covert) of an individual or groups (in case of demonstrations for example) and be extremely versatile (can go almost anywhere), they offer a superior level of surveillance. For example, they can fly over closed gardens, follow individuals on the streets, detect and count how many individuals there are in a building or in a particular room. The technology they can transport and the fact that they can be either big and visible or small and quasi invisible (surreptitious, clandestine) can make them highly intrusive.

20. As a result, most of the various uses of RPAS described in paragraph 15 of this Opinion (filming, audio recording, biometric sensors…) constitute an interference

[17] For example, see http://www.mmu.ac.uk/news/news-items/2211/

[18] 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 an on the free movement of such data.

with the right to the respect for private and family life guaranteed by Article 8 of the Council of Europe Convention on Human Rights (hereinafter "ECHR") and Article 7 of the Charter of Fundamental Rights of the European Union (hereinafter "the Charter"). Furthermore, since most of these uses include the processing of personal data, the conditions for such processing laid down in Article 8 of the Charter must also be respected.

21. Consequently, it is of crucial importance that, as underlined by the Communication, RPAS are developed on the EU market in full compliance with the fundamental right to the respect for private and family life guaranteed in Article 8 of the ECHR and Article 7 of the Charter and with the right to the protection of personal data, as guaranteed in Article 8 of the Charter.

22. Data protection law establishes a number of requirements and safeguards, which enable the controller to process personal data, provided that RPAS are used transparently and for lawful purposes, and that they raise individuals' awareness on the actions carried out through RPAS when they involve processing of their personal data. Because RPAS are remotely piloted, controllers should not only focus attention on the act of piloting but should also point out their possible consequences. The consideration of individuals' rights to privacy and data protection should raise their awareness on the consequences of their acts.

II.3. Consequence: the use of RPAS for civil purposes must comply with fundamental rights to privacy and data protection

23. The use of RPAS for civil purposes must comply with the fundamental rights to privacy and data protection. The EDPS therefore welcomes the reference in the Communication to the EU data protection legal framework and the insertion of a chapter 3.4 dedicated to fundamental rights. In this part of the Opinion, we will further explain this framework and its application to the variety of situations where RPAS can be used.

The rights to privacy and data protection are fundamental rights granted to individuals in the EU

24. As noted above, the right to privacy is a fundamental right enshrined in Article 8 ECHR and article 7 of the Charter. Any interference with this right should only be allowed in accordance with Article 8(2) of the ECHR and Article 52(1) of the Charter[19].

25. Besides, the fundamental right to data protection, enshrined in Article 8 of the Charter and Article 16 of the Treaty on the Functioning of the EU (hereinafter: "the TFEU"), applies to the processing of personal data. Member States and the EU institutions have a positive obligation to ensure that, be it for commercial or professional, law enforcement, intelligence or private purposes, the processing of personal data *via* RPAS respects the essential elements set forth in Article 8 of the Charter as well as the more detailed rules laid down in EU secondary legislation.

26. Under secondary law, Directive 95/46/EC, Council Framework Decision 2008/977/JHA[20], Regulation (EC) 45/2001 and Directive 2002/58/EC,[21] as interpreted by the Court of Justice of the EU (hereinafter "CJEU"), lay down detailed conditions and safeguards to ensure the lawful processing of personal data. Council of Europe Convention 108 for the protection of individuals with regard to automated processing of personal data also provides relevant safeguards.

27. The articulation of these legal rights with the different possible purposes for which personal data can be processed using RPAS will be explained in the following paragraphs.

Expectations of privacy and protection of one's personal data in the public space in the EU

28. In the EU, unlike other jurisdictions[22], the location in a public or private space is not a relevant criterion when determining whether the right to privacy and the right to data protection apply or not.

29. As recalled by the European Court of Human Rights in its *Von Hannover v. Germany* ruling[23], "*the concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings.* ***There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life.*** *Publication of a photo may thus intrude upon a person's private life even where that person is a public figure*"[24]. The Court reiterated that, "*in certain circumstances, even where a person is known to the general public, he or she may rely on a "legitimate expectation" of protection of and respect for his or her private life*"[25].

30. As a result, individuals in a public space, both private individuals and public figures, can still assert, for example, their right to respect for their private and family life, i.e. the right not be targeted with a zoom lens or a directional microphone or to protection against the exposure of the totality of their movements to the public, being tracked or the recording of their conversations.

[20] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
[21] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[22] See US case law developed on aerial surveillance according to which the police can validly fly over a garden and spot elements constituting part of a criminal offence. There is no intrusion into the person's privacy because 'any member of the public flying in this airspace who glanced down could have seen everything that these officers observed." US Supreme Court, 1986, California v. Ciraolo.
[23] Applications nos. 40660/08 and 60641/08, *Case of Von Hannover v. Germany (No. 2)*, Judgment of the Grand Chamber of the European Court of Human Rights of 7 February 2012.
[24] See paragraph 95 of the aforementioned judgment.
[25] See paragraph 97 of the aforementioned judgment.

31. In parallel, the processing of personal data triggers the application of the European data protection framework, wherever it is carried out, whether in a public or a private space, as long as the processing takes place in the context of the activities of an establishment of the controller in the EU or with equipment or means located in the EU[26].

32. Even though technological developments would allow a significant increase in surveillance of individuals in the public space or even in private spaces (such as their house, balconies or garden) and the processing of a larger amount of personal data, these rights would remain and the safeguards they represent would not be lowered.

Applicability of the data protection framework to the use of RPAS for private activities, in particular by hobbyists

33. The right to data protection does not apply in the limited number of exceptions in Article 3(2) of Directive 95/46/EC. Amongst these, the household exception could be relevant to a few limited uses of RPAS. The right to data protection is thus excluded when the processing of personal data is strictly limited to processing by a natural person in the course of a purely personal or household activity. Recital 12 refers to activities which are exclusively personal or domestic, giving correspondence and the holding of records of addresses as examples of activities excluded from the scope of the Directive.

34. In its judgment in the *Bodil Lindqvist* case[27], the CJEU clarified that the exception provided for in the second indent of Article 3(2) of Directive 95/46 relates "*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*".

35. Consequently, the processing of personal data through RPAS carried out by private users would not fall within the household exception in cases where the use of the RPAS is aimed at sharing or even publishing the resulting video/sound captures/images or any data allowing the direct or indirect identification of an individual on the Internet and, consequently, to an indefinite number of people (for instance, via a social network).

36. Besides, in the annex to its Statement on current discussions regarding the data protection reform package[28], the Article 29 Working Party proposed a set of criteria to help determine whether or not a processing is done for personal or

[26] See Article 4(1)(a) and (c) of Directive 95/46/EC.
[27] Case C-101/01, *Bodil Lindqvist*, judgment of 6 November 2003, paras 46-47.
[28] Statement of the Working Party on current discussions regarding the data protection reform Package, 27.02.2013, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_reform_package_en.pdf

household purposes[29]. When applying those criteria to RPAS, it can often be concluded that in many cases the household exception would not apply.

37. As stated in the document, "*none of these criteria are, in themselves, necessarily determinative. However, a combination of these factors shall be used to determine whether or not particular processing falls within the scope of personal or household processing*". To this aim, one must determine:
    - if the personal data is disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances,
    - if the personal data is about individuals who have no personal or household relationship with the person posting it,
    - if the scale and frequency of the processing of personal data suggest professional or full-time activity,
    - if there is evidence of a number of individuals acting together in a collective and organised manner,
    - if there is a potential adverse impact on individuals, including intrusion into their privacy.

38. Submitting the use of RPAS by private users/citizens for private activities or as a hobby, and the resulting processing of personal data, to these criteria, one comes to the conclusion that the processing carried out *via* RPAS might meet several of these criteria and fall out of the scope of the household exception. For example, personal data might be disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances. This was for example the case when a film of a French city recorded via RPAS was posted on a video sharing website. In addition, if RPAS were to be used for private purposes in public areas, it is likely that many individuals with no personal relationship with the pilot will see their data collected or even with the individuals accessing the data. The scale and frequency might vary a lot depending on hobbyists who could join clubs and associations and sometimes, but not necessarily and systematically, act in a collective and organised manner. The last criterion is even more relevant since there is an undeniable potential adverse impact on individuals, i.e. the intrusion into their privacy.

39. As a result of this analysis, RPAS uses by individuals for private activities may, quite frequently, be subject to the requirements of Directive 95/46/EC. In any event, as a pre-condition for the data protection rules, the processing of personal data must be lawful in all respects. This means also complying with other relevant rules in areas such as civil or criminal law, intellectual property, aviation or environmental law.

Applicability of the data protection framework to the use of RPAS for commercial or professional and administrative purposes

40. The processing of personal data *via* an RPAS for commercial or professional purposes must comply with national legislation implementing Directive 95/46/EC

[29] Annex 2, Proposals for Amendments regarding exemption for personal or household activities, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf .

if the controller is established on the EU territory or is making use of equipment situated on the territory of an EU Member State[30]. The territorial scope of application of the directive was recently clarified by the CJEU in its judgment *Google Spain v AEPD*[31]. In that judgment, the Court took into account a number of elements, such as the presence of an establishment on the territory of an EU Member State and the relationship between the activities of that establishment and the data processing at issue, to decide on the applicability of EU data protection law to a processing carried out online by a company having its principal establishment outside the EU. Article 3 of the proposed General Data Protection Regulation[32] (hereinafter "GDPR"), which is still under negotiation, would extend this scope to the processing of personal data "*in the context of the activities of an establishment of a controller or a processor in the Union*"[33] and "*to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour*"[34].

41. RPAS manufacturers and controllers therefore have to take account of the requirements laid down in applicable data protection law as well as best practices deriving from the applicable data protection framework, in particular they should implement privacy by design and by default and carry out data protection impact assessments (hereinafter "DPIAs") where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. These practices should all the more be taken into account considering that they not only derive from obligations set forth in the current framework but also that they will be clearly stipulated in the proposed GDPR[35] which will replace the current framework.

Applicability of the data protection framework to the use of RPAS for journalistic purposes

42. Article 9[36] and recital 17 of Directive 95/46/EC refer to the processing of personal data for journalistic purposes, setting a possibility for Member States to provide for

[30] As laid down in Article 4(1) of Directive 95/46/EC. Pursuant to Article 4(1)(c), the use of equipment on the EU territory for purpose of processing personal data must comply with the national data protection rules in that jurisdiction. This may have consequences for transnational operated drones, in particular as regards the question of whether the drone is used as equipment as a means for processing personal data on EU territory. For further guidance, see Article 29 Working Party Opinion 8/2010 on applicable law, adopted on 16.12.2010.

[31] Case C-131/12., *Google Spain SL, Google Inc.v Agencia Española de Protección de Datos (AEPD),* judgment of the Court of 13 May 2014.

[32] COM(2012) 11 final, 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 (General Data Protection Regulation), 25.1.2012.

[33] See GDPR Article 3(1).

[34] See GDPR Article 3(2).

[35] See GDPR Article 30(3) for privacy by design and by default and Article 33 on data protection impact assessments.

[36] Article 9 of Directive 95/46/EC states that : *"Processing of personal data and freedom of expression Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic*

exemptions or derogations from the provisions of its Chapter II on the lawfulness of the processing of personal data, Chapter IV on the transfer of personal data to third countries and Chapter VI relating to the supervisory authority and Working Party on the protection of individuals with regard to the processing of personal data, if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

43. Nevertheless, as clarified by the CJEU in the *Satamedia* ruling[37], "*activities […] may be classified as 'journalistic activities' if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them*". The mere publication of data on the Internet or in a newspaper, without such an object is not sufficient for it to fall under the journalism exception.

44. The use of RPAS for journalistic purposes will therefore fall under the national measures implementing this Article. To avoid cross-border issues that may emerge due to discrepancies, the EDPS would advise that the Commission work closely with the Article 29 Working Party on guidance specifically related to the use of RPAS by journalists. However, this conclusion might not entirely apply if the national measures were not aimed at the processing of personal data, whether or not for journalistic purposes, but at the use of RPAS as such in general.

Applicability of the data protection framework to the use of RPAS for law enforcement purposes

45. Law enforcement authorities processing personal data *via* RPAS have to respect the fundamental right to privacy as enshrined in Article 8 of the ECHR and the interference with the exercise of this right should be done in accordance with Article 8(2) of the ECHR and the corresponding case law of the the European Court of Human Rights. As a result, their activities must take place in accordance with the law, i.e. be based on a law or prescribed by law, this law being publicly accessible so that citizens are able to obtain information on how their rights may be interfered with. This law should also be foreseeable, meaning sufficiently clear and detailed for the citizen to be able to foresee when he or she is likely to be subjected to measures involving RPAS. The methods and types of uses of RPAS by law enforcement authorities should not be secret. This use should serve one of the legitimate goals set out in Article 8 paragraph 2 of the ECHR and be necessary in a democratic society, that is respond to a "pressing social need". The ECtHR applied these requirements to the interference of law enforcement authorities with the exercise of the right to privacy in its *S. and Marper* ruling[38].

46. Law enforcement's processing of personal data also fall under Articles 7 and 8 of the Charter and Article 16 TFEU. These instruments set forth requirements for protecting the fundamental rights to private and family life and to data protection, which are complemented by more detailed rules in EU secondary legislation. For

---

purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression".

[37] See paragraph 61 of case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy*, judgment of the Court (Grand Chamber) of 16 December 2008.

[38] Applications nos. 30562/04 and 30566/04, case of *S. and Marper v. the United Kingdom*, judgment of the Grand Chamber of the ECtHR of 4 December 2008.

example, if RPAS are used in the framework of police and judicial cooperation in criminal matters, any exchange between Member States of personal data gathered through RPAS will have to comply with their requirements as specified in Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[39].

47. More detailed rules can also be found in specific international instruments to which all EU Member States are a party. In particular, insofar as personal data are being processed, the requirements set forth in the Council of Europe Convention 108 and in Recommendation n° R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector must be complied with by the authorities processing personal data for law enforcement and national security uses.

48. As a result, any intrusive processing by law enforcement authorities must be subject to the necessary data protection safeguards recalled by the CJEU in the *Digital Rights Ireland* ruling[40].

49. In particular, it should be ensured that law enforcement authorities only use an RPAS in the framework of a specific investigation when their use is considered necessary and where no other less intrusive mean would achieve the same purpose. We would also draw attention to data protection restrictions on automatically enforced decisions.

Applicability of the framework to the use of RPAS for intelligence services

50. According to Article 4(2) of the Treaty of the European Union (hereinafter: "TUE"), "national security remains the sole responsibility of each Member State. The CJEU has confirmed that the use of RPAS for purposes outside the scope of the Treaty, such as intelligence, should none the less comply with the key principles of necessity and proportionality laid down in Article 8 of the ECHR as interpreted by ECtHR case law (see above)[41]. Besides, the exception laid down in Article 4(2) must be interpreted strictly[42], so that activities by intelligence agencies which fall within the scope of EU law (e.g. surveillance for foreign policy, law enforcement or purely commercial purposes) must respect these principles.

51. This was recalled by the EDPS in the Opinion on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows"[43], by stating that: "*At the moment of implementing a*

[39] See however the explanatory memorandum of the European Commission to the Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data /* COM/2012/010 final - 2012/0010 (COD). In particular, page 2 paragraph 2.
[40] Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*.
[41] Judgment in Joined Cases C-465/00 C-138/01 and C-139/01, *Rundfunk*, paras 72 and 91.
[42] Judgment in Case C-222/84, *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary*.
[43] See EDPS Opinion of 20 February 2014 on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the

surveillance activity which involves a new processing operation, the need for an authorisation of the activity by a judge or another independent authority would reduce the risk of abuse by ensuring that necessity and proportionality are determined at the moment that decisions are taken that affect the private life of citizens. The authorisation should contain an assessment of the necessity and proportionality of the measure, provide for appropriate safeguards where necessary, and be limited in time[44]".

52. The Article 29 Working Party has also highlighted[45] that "*under no circumstance surveillance programmes based on the indiscriminate, blanket collection of personal data can meet the requirements of necessity and proportionality set out in these data protection principles. Limitations to fundamental rights have to be interpreted restrictively, following case law from the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (ECJ). This includes the need for all intrusions to be necessary and proportionate in relation to the purpose to be achieved*".

III. SPECIFIC COMMENTS

53. The EDPS wishes to address these specific comments to the Commission to help a swift introduction of RPAS on the EU territory based on the assurance that future policy making decisions or measures relating to RPAS integrate data protection and privacy requirements.

III.1. Scope of EU policy action on RPAS

54. The Commission is currently not competent for the regulation of RPAS under 150 kilos[46], the European Aviation Safety Agency only being competent for the regulation of RPAS above 150 kg. Still, as abovementioned, RPAS operations, whatever the weight of the aircraft, are subject to the European and EU data protection framework and the national legislation implementing it to the extent that they involve the processing of personal data. In this respect, the EU should play a leading role in raising awareness of manufacturers, users and data subjects on the existing data protection framework, regardless of the size of the RPAS.

Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf .

[44] See paragraph 75 of the abovementioned Opinion.

[45] See opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Adopted on 10 April 2014, 819/14/EN WP 215, page 6 available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf .

[46] See in particular EU Regulation on common rules in the field of civil aviation currently only applies to RPAS above 150 kg and its annex II See annex 2 Aircraft referred to in Article 4(4) of 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, (i)" Article 4(1), (2) and (3) do not apply to aircraft falling in one or more of the categories set out below:[…] unmanned aircraft with an operating mass of no more than 150 kg;".

55. In view of the imperative need to ensure respect for privacy, data protection and security requirements relating to this potentially highly intrusive new technology, the EDPS welcomes that the Communication states that the current scope of EU policy action on RPAS should be "reconsidered"[47]. In effect, the threats arising from mobility and discretion discussed in paras 17-19 apply in particular to smaller and lighter RPAS which potential proliferation calls for the harmonisation of the rules applying to them. If the Commission were to adopt policy measures in the field of RPAS, including on light RPAS, those measures should take into account applicable data protection law and the general obligations under Articles 7 and 8 of the Charter so as to embed the necessary and appropriate safeguards.

56. Moreover since data protection obligations can be most effectively ensured by considering them from the outset, applying the principle of privacy by design, rather than retrofitting them later, the Commission should also encourage RPAS manufacturers to implement them. The principle of privacy by design is one of the key obligations which will be introduced in the General Data Protection Regulation as mentioned above[48]. The EDPS would favour encouraging compliance by manufacturers in order to ensure that RPAS are designed in a manner that appropriately embeds data protection requirements (see further comments in III.2 below).

III.2. Generate a public debate by raising awareness on the privacy implications of the use of RPAS

57. The EDPS welcomes the initiatives and awareness raising projects that should accompany the introduction of RPAS on the EU civil market. It is vital to raise public awareness of the implications of RPAS for privacy and data protection and of the obligations with which manufacturers, controllers, processors and users must comply.

58. In this respect, we would underline the work already being done by some national data protection authorities on the impact of RPAS on the right to respect for privacy and data protection[49].

59. Besides, both the EDPS and the Article 29 Working Party have been associated at an early stage to the reflection conducted by the Commission on RPAS. The EDPS would like to continue this close cooperation with the Commission in the framework of the Article 29 Working Party in order to ensure, in a harmonised manner, that RPAS are used in compliance with the applicable data protection requirements.

III.3. Support implementation of privacy by design by RPAS manufacturers

[47] See page 5, part 3.1.
[48] See paragraph 41,
[49] The CNIL published a research document on drones at the end of 2013 on this issue, the UK Information Commissioner is currently conducting a consultation to update its CCTV code of practice which now includes a section dedicated to drones and the Belgian data protection authority has published FAQs on this same issue in April 2014.

60. RPAS that are to be operated on the EU territory need to integrate, at practical level, data protection and privacy from their very inception. This has to be done taking account of the specificities of RPAS: in effect, they consists of an aerial vehicle, the carrier, and a payload which may be a data processing system and both parts can be produced by completely different manufacturers, who may not even be aware of the later combination and its capabilities. In this perspective, the Commission should encourage manufacturers to take privacy by design into account whenever the product being designed has a known potentially privacy-intrusive use, e.g. by producers of complete monitoring or surveillance systems and by producers of bolt-on systems. This is all the more a sensible course of action because privacy by design will be become a specific legal requirement under the GDPR[50]. Later on, when the combination done by the user and the modalities of use of the RPAS result in privacy-intrusive acts, the final responsibility will be with the user.

61. RPAS manufacturers should be invited to analyse at the earliest stages of development how their device might interfere with individuals' privacy, so that they may then build these devices[51] in a way which reduces such interference to what is strictly necessary and proportionate to the lawful purpose pursued. In the case of RPAS, the Commission should recommend RPAS manufacturers to:
    - Propose different categories of sensors depending on private sector buyers' business objective, so that the later can choose the one which would affect privacy the least (for example, an RPAS used in order to build accurate roadmaps probably does not need a high resolution camera capable of discerning license plates of vehicles);
    - Set up data retention by design, that is the possibility to schedule the automatic and regular deletion of the data processed;
    - Provide tools with data protection friendly functionalities such as the possibility to turn on and off sensors in flight (so that the recording is not continuous but triggered only when necessary and proportionate to the purpose pursued), automatic masking of private areas, automatic detection and pixelation of faces that are accidentally gathered in images and videos[52];
    - Configure by default any functionality provided by the devices to the most privacy-friendly settings;
    - Provide clear information to the user on privacy issues that may arise when using the device, possibly in a privacy notice accompanying all RPAS sold within the EU territory.

III.4. Assist controllers with compliance

62. Regarding the sale of RPAS to private or professional end users, the EDPS would recommend that any future policy measure at EU level to facilitate those sales (such as type approval regulation) would require inserting "privacy notices" in packages for small RPAS. Those privacy notices would recall data protection/privacy requirements applicable to personal data processing carried out

[50] See Article 30(3) of the GDPR.
[51] The analysis of potential privacy issues is key to the development and use of RPAS and should guide business processes and technological choices.
[52] See The Regulation of the Impact of Civilian Drones on Behavioural Privacy, 3 March 2014, Computer Law & Security Review 30, 3 June 2014, Roger Clarke.

via RPAS operated within the EU and explain practical consequences such as, where applicable, the obligation to carry out a data protection impact assessment, , the obligation to inform individuals about the processing of their personal data, the possible obligation to notify the data processing to the competent data protection authority, and the need to easily identify the person operating the RPAS.

63. In any case, the EDPS would insist that RPAS users (citizens, companies, administrations, professionals, law enforcement, intelligence services…) should be aware of the privacy impact of their actions, analyse their needs and implement processes surrounding the use of the RPAS in such a way that privacy is impacted the least[53]. This would typically require that they carry out a data protection impact assessment. To mirror the privacy by design requirements on manufacturers, users should, at a minimum:

- Define a purpose for their use in order to prevent the risks of function creep and collect only the data strictly necessary for this purpose, in line with the data minimisation principle. Limits should be set to potential constant tracking via RPAS. Data subjects should be appropriately informed on the use of RPAS and on modalities to exercise their rights;
- Choose the right tool for the job, i.e. not choosing RPAS overloaded with high resolution sensors if those are not needed to meet the objectives of the user;
- Configure their device taking the most privacy-friendly approach, i.e. any privacy-friendly functionality designed into the device should be set to the strictest parameters that would fulfil the needs of the user and affect privacy the least (e.g. short retention periods, masking of private areas, pixelation of faces that are accidentally gathered in images and videos, sensors turned on only when necessary);
- Manage the security of any collected data appropriately.

64. Further action is also needed to encourage measures that would facilitate identification of the controller of an RPAS.

IV. CONCLUSIONS

65. The EDPS welcomes the fact that he has been consulted by the Commission on this Communication and highlights that civil uses of RPAS cover all areas not covered by military uses, thus not limited to commercial uses. He also welcomes that the Communication not only underlines the social and economic benefits of the civil use of RPAS but also identifies privacy, data protection and security as key elements with which to ensure compliance for their dissemination.

66. RPAS should be distinguished from aeroplanes and CCTV because their "mobility and discretion" enable them to be used in many more circumstances. Besides, they can be combined with other technologies such as cameras devices, Wi-Fi sensors, microphones, biometric sensors, GPS systems, systems reading IP addresses, RFID

[53] The analysis of potential privacy issues is key to the development and use of RPAS and should guide business processes and technological choices.

tracking systems which all offer the possibility to process personal data and make same potentially powerful surveillance tools.

67. The EDPS would therefore underline that RPAS uses involving the processing of personal data constitute in most cases an interference with the right to the respect for private and family life guaranteed by Article 8 of the Council of Europe Convention on Human Rights (hereinafter "ECHR") and Article 7 of the Charter of Fundamental Rights of the European Union (hereinafter "the Charter") as they challenge the right to intimacy and privacy guaranteed to all individuals in the EU and can therefore be allowed only under specific conditions and safeguards. In any event, whenever personal data are processed by RPAS operated in the EU, which is common, the right to the protection of personal data enshrined in Article 8 of the Charter applies and the EU legal framework for data protection should be complied with.

68. In practice, therefore, RPAS uses by individuals, for private activities will normally be subject to Directive 95/46/EC requirements and will rarely benefit from the household exception. In any event, as a pre-condition for the data protection rules, the processing of personal data must be lawful in all respects. This means also complying with other relevant rules in areas such as civil or criminal law, intellectual property, aviation or environmental law.

69. The processing of personal data *via* an RPAS for commercial or professional purposes must comply with national legislation implementing Directive 95/46/EC.

70. Moreover, the EDPS would recall that the mere publication of data on the Internet or in a newspaper, without any aim to disclose to the public information, opinions or ideas, is not sufficient for it to fall under the journalism exception of Article 9 of Directive 95/46/EC.

71. Law enforcement uses of RPAS also have to respect the fundamental right to privacy so that these activities should be based on a clear and accessible law, serve a legitimate goal and be necessary in a democratic society and proportionate to the purpose pursued. When they result in processing personal data, they are subject to the data protection safeguards laid down at EU and Council of Europe level.

72. The use of RPAS for intelligence purposes must respect the principles of necessity and proportionality.

73. In view of the imperative need to ensure respect for privacy, data protection and security requirements relating to this potentially highly intrusive new technology, the EDPS supports the Commission reconsidering its lack of competence for the regulation of RPAS under 150 kilos.

74. The EDPS also welcomes the initiatives and awareness raising projects that should accompany the introduction of RPAS on the EU civil market.

75. The EDPS recommends that the Commission encourages RPAS manufacturers to implement privacy by design and by default and data controllers to carry out data protection impact assessments where processing operations present specific risks to

the rights and freedoms of data subjects by virtue of their nature, scope or purposes.

76. Further action is also needed to encourage measures that would facilitate identification of the controller of an RPAS.

Done in Brussels, 26 November 2014

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor