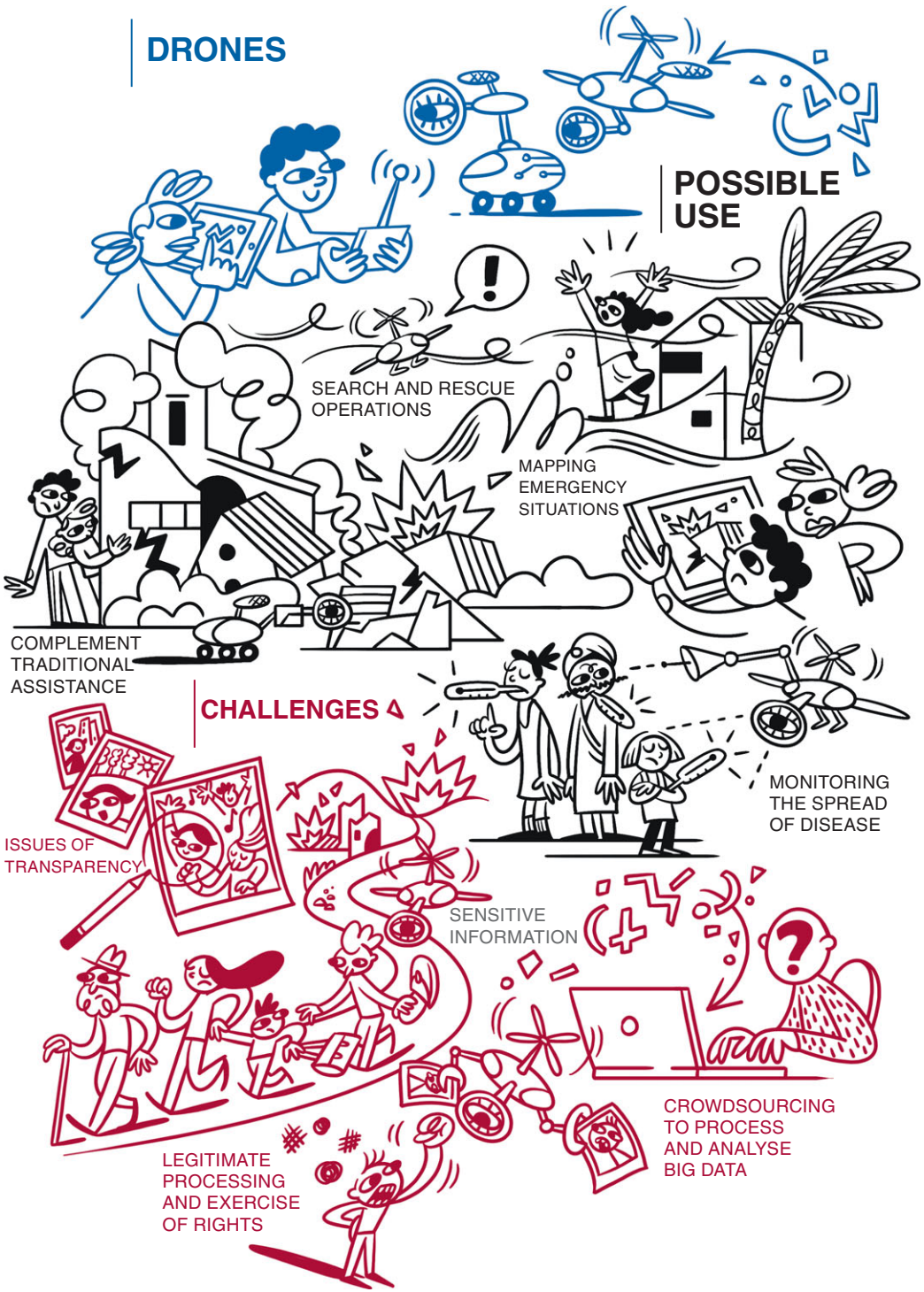

CHAPTER 7

DRONES/UAVS AND REMOTE SENSING

Massimo Marelli

7.1 INTRODUCTION

Drones are a promising and powerful technology potentially capable of helping Humanitarian Organizations to improve their situational awareness, their response to natural and man-made disasters, and their relief operations. They can complement traditional manned assistance by making operations more efficient, effective, faster and safer. If deployed correctly, Drones could have a significant impact on Humanitarian Action.

Drones are small aerial or non-aerial units that are remotely controlled or operate autonomously. They are also known as Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Aircraft Systems (RPAS). Depending on what they are used for, they are often equipped with cameras, microphones, sensors or GPS devices, all or any of which may make Personal Data Processing possible.

From a data protection perspective various concerns have been raised about the use of Drones. However, it is important to clarify at this early stage that what is of interest in the case of Drones is not their use *per se*, but the different technologies they are equipped with, such as high-resolution cameras and microphones, thermal imaging equipment or devices to intercept wireless communications, because it is these technologies that are used for data collection and Processing. In this respect, the considerations addressed in this chapter could also apply to the use of satellites and, more generally, to remote sensing.

This chapter focuses only on the data protection issues posed by the use of Drones. Other issues and fields of law may be relevant, but will not be dealt with. For instance, guidance will not be provided on air traffic control issues, flight licences, equipment safety certificates or similar matters.

In general terms, the most common humanitarian use of Drones today entails observation and data collection to enhance situational awareness. Below is an indicative list of the applications for which Drones are or could be used in a humanitarian setting:

- search and rescue;
- determining the whereabouts of people unaccounted for;
- collection of aerial imagery/situation awareness/post-crisis assessment (e.g. surveying the condition of power lines and infrastructure, assessing the number of wounded people, destroyed homes, dead cattle, etc.);
- monitoring the spread of a disease through the use of heat sensors;
- mapping emergency housing settlements;
- real-time information and situation monitoring, by providing videos or photos and thus giving an overview;

- locating unexploded ordnance (UXO);
- mapping natural disasters or conflict sites;
- locating and following people displaced by a Humanitarian Emergency;
- delivery of medicines/other rescue equipment in remote areas;
- setting up a mesh network/restoring communication networks by relaying signals.

In disaster situations "drones may be used to provide relief workers with better situational awareness, as they can locate survivors amidst the rubble, perform structural analysis of damaged infrastructure, deliver needed supplies and equipment, evacuate casualties, and help extinguish fires – among many other potential applications".[1] Drones can also supply aerial data from areas which are considered unsafe for Humanitarian Action providers (e.g. sites contaminated by radioactivity or wildfire locations).[2]

Nevertheless, while Drones may be an invaluable source of direct and indirect information when responding to emergencies, a critical assessment has to be made before they are used in any particular case. Their use may include significant risks.[3] Apart from safety issues *per se* (e.g. accidents during their deployment that could result in bodily injury or even death), they may be perceived as spying or intruding in a conflict scenario, something that could severely compromise the safety of their operators and the staff of Humanitarian Organizations, as well jeopardizing local people who may be perceived by the parties in the conflict as having given Consent to the use of Drones on their behalf.

EXAMPLE:
A Humanitarian Organization may have acquired the approval of local community leaders for Drones to be used for the provision of aerial imagery over a large geographical area. However, during its deployment a Drone may accidentally photograph, and consequently provide evidence of, illegal activity taking place in some specific place in the above-mentioned geographical area. The groups carrying out the illegal activity, aware of the Drone flying over them, may seek to find and punish the

1 Joint Legislative Committee on Emergency Management and the Senate Committee on Judiciary, *Drones and Emergencies: Are We Putting Public Safety at Risk?*, in Oversight Hearing, Background Paper, California State Senate, 2015, 10: https://sjud.senate.ca.gov/sites/sjud.senate.ca.gov/files/background_paper_-_drones_and_emergencies.pdf.

2 American Red Cross, *Drones for Disaster Response and Relief Operations*, ed. Measure, a 32 Advisors Company, April 2015: www.issuelab.org/resources/21683/21683.pdf.

3 Florian Delafoi, "Le drone, l'allié ambigu des humanitaires", *Le Temps*, 11 April 2016, Online edition: www.letemps.ch/monde/drone-lallie-ambigu-humanitaires; ICTworks, "What Do Tanzanians Think about Drones? Now We Know", ICTworks (blog), 22 February 2016, www.ictworks.org/what-do-tanzanians-think-about-drones-now-we-know.

community leaders who provided their approval and also seek the Humanitarian Organization's operators in order to destroy the evidence collected.

As noted above, concerns about potential violations of Personal Data protection rights are not caused by the use of Drones, but rather by the on-board equipment which can process Personal Data. Information technologies embedded in Drones or connected to them can perform various data Processing activities and operations (e.g. data collection, recording, organization, storage and combination of collected data sets). Data typically collected by Drones include video recordings, "images (e.g. 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".[4] Depending on the quality of the data, it may be possible to identify individuals directly or indirectly. This can be done either by a human operator or automatically, for instance by capturing an image from a facial recognition program/algorithm, scanning to detect a smartphone and using it to identify the person or using radio-frequency identification (RFID) chips in passports.[5]

The following factors may be relevant while assessing Humanitarian Organizations' data protection response to the use of Drones:

- It is technically possible to make aerial Drones flight-specific, on the basis of unique identifiers embedded in their basic equipment.
- Permission to fly Drones and a remote pilot's licence issued by the state authorities are required in many countries.[6]
- Imagery data (of various levels of analysis and quality) are the most common type of data collected by Drones.
- Altitude of flight and angle of capture of the imagery also have a significant impact on the likelihood that the imagery captured may directly or indirectly identify an individual.
- Although technology is advancing rapidly, at present Drones can capture extremely detailed pictures, but most cannot capture individuals' faces. The picture has to be connected to other data sets in order to lead to identification. When facial identification is not possible, identification may be possible through the use of location and other types of data. The use of metadata (data that provide information about other data) is crucial in this context.

4 Article 29 Data Protection Working Party, *Opinion 01/2015 on Privacy and Data Protection Issues Relating to the Utilisation of Drones*, European Commission, 23 November 2016, 7: https://ec.europa.eu/newsroom/article29/items/640602.

5 Ibid., 14.

6 Storyhunter, "Storyhunter Guide to Commercial Drone Regulations around the World", Medium (blog), 3 April 2018: https://blog.storyhunter.com/storyhunter-guide-to-commercial-drone-regulations-around-the-world-5795c31165d9.

- It is important to establish where data collected are kept and what types of Processing are performed on them; in this respect there is a correlation between Drones and the use of Data Analytics.[7]
- A number of international initiatives on standards and other Drone-use specifications are currently under way, some looking specifically at the use of Drones for humanitarian purposes. Humanitarian Organizations are advised to follow these initiatives closely and apply their findings in their practices.[8]
- Humanitarian Organizations often outsource their drone operations to professionals, which therefore raises specific data protection issues (e.g. Data Controller/Data Processor relationship, access to data, etc.).
- Drone-related Personal Data Processing often involves cross-border transfers, which require a legal basis under data protection law.

However, it is worth noting that, given the pace of change in these technologies, a number of the above findings may change substantially in the near future.

Humanitarian Organizations should also take into account that, even when identification of individuals is not possible via the use of Drones, their use may still have substantial implications for the life, liberty and dignity of individuals and communities. Humanitarian Organizations should accordingly take precautions to protect Drone-collected data, even if the individuals recorded in them are not immediately identifiable.

EXAMPLE:
If the data from tracking streams of displaced people with Drones are accessed by ill-intentioned Third Parties, vulnerable individuals can be put at risk, even if they cannot be individually identified.

7.2 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.

7 See Chapter 17: Artificial Intelligence.

8 See for example: "Guidelines", Humanitarian UAV Code of Conduct (blog), 6 December 2017: https://uavcode.org/further-guidance; "Humanitarian UAV Guidelines on Data Protection", Humanitarian UAV Code of Conduct (blog), 6 December 2017: https://uavcode.org/further-guidance/131-2.

7.2.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations can process Personal Data collected by Drones using one or more of the following legal bases:[9]

- the vital interest of the Data Subject or of another person;
- the public interest, in particular stemming from an organization's mandate under national or international law;
- Consent;
- a legitimate interest of the organization;
- the performance of a contract;
- compliance with a legal obligation.

Lawfully acquiring Consent will most likely prove unrealistic in practice for work carried out by Humanitarian Organizations using Drones.

For example, Consent would not be "freely given" whenever an individual is not free to enter or leave a surveyed area.

This means that Consent as a lawful basis for Personal Data Processing in the context of Drone operations by Humanitarian Organizations seems to be generally unrealistic. Drones are used in most cases where there is limited or no access to communities. Even if such access was provided, it would still be almost impossible to obtain Consent from all the people who may potentially be affected by the Drone-related Processing. In addition, depending on the circumstances in which Drones might be used, it is questionable whether Consent from people in distress and in need of humanitarian assistance could be considered free.

The idea of acquiring the "Consent of the community" or the "Consent of authorities" has also been suggested for the use of Drones in Humanitarian Action as a plausible alternative to individual Consent. This could involve, for example, obtaining Consent only from representatives of a group of vulnerable individuals and not the individuals themselves. However, under data protection law Consent must be provided by the individual in order to be used as a valid legal basis.

EXAMPLE:
Community leaders or the state authorities concerned could give their Consent to the use of Drones by a Humanitarian Organization in order to map a refugee camp, but the individuals present in the area may not be aware of the Drones, or not wish to be photographed/have their Personal Data collected by Drones.

9 See Chapter 3: Legal bases for Personal Data Processing.

Where Consent cannot be obtained from the individual concerned, Personal Data can still be processed by the Humanitarian Organization if it establishes that Processing may be in the vital interest of the Data Subject or of another person, or if another legal basis applies (as noted in Section 7.2.1). In other words, Personal Data can be processed where the Processing is necessary in order to protect an interest which is essential for the Data Subject's life, integrity, health, dignity or security or that of another person.

As has already been mentioned in Chapter 3: Legal bases for Personal Data Processing, given the nature of Humanitarian Organizations' work and the emergency situations in which they operate, in some circumstances there may be a presumption that the Processing of data necessary for humanitarian purposes is in the vital interest of a Data Subject.[10]

The use of Drones by Humanitarian Organizations should be assessed in each particular case to determine whether it is actually necessary for the protection of the vital interests of the Data Subject or another person. The Drones' contribution to the protection of overriding private interests such as life, integrity and security has to be proven or, at least, be probable given the type and scale of the emergency, or concerns about a lack of information relating to the emergency, which could only be remedied by the use of Drones. Strict standards should therefore be applied to determine whether this legal basis is present.

EXAMPLES:

- The use of Drones in search and rescue operations by a Humanitarian Organization would most likely qualify under this legal basis, because it would protect the vital interest of the Data Subject (i.e. the person unaccounted for).
- The use of Drones in mapping operations by a Humanitarian Organization, in the absence of a specific emergency, would most likely not qualify under this legal basis, because there is no direct connection with the vital interests of the Data Subjects living or moving around in the areas being mapped.

It is important for Humanitarian Organizations to make careful assessments when important grounds of public interest are triggered and are to be used as a lawful basis for Processing Personal Data collected by Drones. For example, this will usually be the case when the activity in question is an important part of a humanitarian mandate established under national or international law (e.g. for the ICRC, IFRC, National Red Cross and Red Crescent Societies, UNHCR, UNICEF, WFP or IOM).

10 See EU, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, Recital 46.

Humanitarian Organizations may also process Personal Data collected by Drones where this is in their legitimate interest, and provided that this interest is not overridden by the Data Subjects' fundamental rights and freedoms. A legitimate interest of an organization can be established when Personal Data Processing is necessary to further or support its mission. It can be argued, however, that where no public or vital interest can be established, it may be difficult to envision circumstances in which the rights and freedoms of the Data Subjects would not override the organization's legitimate interest, particularly in cases where the individuals whose Personal Data are likely to be captured cannot be informed, nor can they effectively exercise their data protection rights.

EXAMPLE:
A Humanitarian Organization may use a Drone to demonstrate successful completion of an action, for instance, to collect footage for a promotional video. This may fall under the legal basis of legitimate interest, although careful consideration of the potential infringement of the rights and freedoms of the individuals appearing in the video would need to be undertaken. In this respect, the extent to which Data Subjects can be informed and effectively exercise their rights (including the right to object) are critical factors.

7.2.2 TRANSPARENCY/INFORMATION

The principle of transparency requires that at least a minimum amount of information concerning the Processing be provided to the Data Subject. In addition, information and communications about the Processing should be easily accessible and easy to understand, expressed in clear and plain language. For obvious practical reasons these requirements can be difficult to satisfy in the case of Drones. Timing of information is also important: in non-emergency situations, this should ideally take place in advance of and during Drone flights. The involvement of community leaders and authorities or media campaigns targeted at the envisaged Data Subjects (e.g. radio, newspapers, and posters in public areas) can help fulfil transparency obligations.

EXAMPLE:
In order to fulfil transparency and information obligations, Humanitarian Organizations using Drones could affix their institutional marks and signs on them; maintain websites or provide relevant information on social media; use available local communication channels (e.g. radio, television, the press); and hold discussions with community leaders.

7.2.3 PURPOSE LIMITATION AND FURTHER PROCESSING

The specific purpose(s) for which Personal Data are collected should be explicit and legitimate. Humanitarian Organizations may use Drones for purposes such as the following:

- search and rescue;
- determining the whereabouts of people unaccounted for;
- collection of aerial imagery, situation awareness, post-crisis assessment (e.g. locating displaced people who need help, surveying the condition of power lines and infrastructure, assessing the number of wounded persons, destroyed homes, dead cattle, etc.);
- monitoring the spread of a disease through the use of heat sensors;
- crowd modelling in protests;
- mapping emergency housing settlements;
- real-time information and situation monitoring, by providing videos or photos and thus giving an overview;
- mapping of natural disasters or conflict sites;
- locating unexploded ordnance (UXO);
- locating and following people displaced by a Humanitarian Emergency;
- delivery of medicines and rescue equipment in remote areas;
- setting up a mesh network or restoring communication networks by relaying signals.

It was also established in Chapter 2: Basic principles of data protection that, irrespective of the legal basis used for the Processing, Humanitarian Organizations may process Personal Data for purposes other than those specified at the time of collection where such Further Processing is compatible with those initial purposes.

7.2.4 DATA MINIMIZATION

Personal Data may only be processed if adequate, relevant and not excessive in relation to the purposes for which they were collected. Therefore, a strict assessment of the necessity and proportionality of the processed data should take place.[11] Moreover, when Drones are used for humanitarian purposes, the principle of data minimization should be respected by choosing proportionate technology and by adopting measures of data protection and privacy by design and by default.

For instance, Humanitarian Organizations could consider the following options:

- Privacy settings on services and products should by default avoid the collection and/or the Further Processing of unnecessary Personal Data.
- Anonymization techniques should be implemented.
- Faces/human beings should be blurred automatically (or only certain particular categories of more vulnerable individuals).

11 See Chapter 2: Basic principles of data protection.

- Flight altitude or angle of capture of imagery should be increased to minimize the likelihood of capturing imagery that can directly identify individuals.

7.2.5 DATA RETENTION

Personal Data processed via Drones should not be stored for a period longer than necessary for the purpose of the Processing. In other words, collected data should be deleted or anonymized when the purpose for which they were collected has been served. The adoption of storage and deletion schedules is also advisable. Data collection devices, carried by Drones or connected to them remotely, should be designed in such a way that, should they need to retain data, a defined storage period for the Personal Data collected can be set and, as a result, Personal Data which are no longer necessary can be automatically deleted according to defined schedules.

EXAMPLE:
Data collected by Drones to help a Humanitarian Organization respond to an incident should, in principle, be deleted when the incident has been dealt with successfully; if the Humanitarian Organization wishes to archive this information (for instance, for historical purposes), it should take adequate measures to protect the integrity and security of the data and to prevent any unauthorized access.

7.2.6 DATA SECURITY

A Humanitarian Organization deploying Drones should implement adequate security measures that are appropriate for the risks involved.[12] For Drones, this could include encryption of databases or temporary storage devices on board, as well as end-to-end encryption of data in transit between the Drone and the base, where applicable.

7.3 RIGHTS OF DATA SUBJECTS

The rights of the Data Subject have already been described in Chapter 2: Basic principles of data protection. The following are some further remarks about Data Subjects' rights with respect to Humanitarian Organizations' use of Drones.[13]

As far as the right to information is concerned, Data Subjects exposed to Drone-related Processing should be provided with the following:

- the identity of the Data Controller of the Drone and of its representative;
- the purposes of the Processing;

12 See Chapter 2: Basic principles of data protection.

13 See Section 2.11 – Rights of Data Subjects.

- the categories of Personal Data collected;
- 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;
- the existence of the right to object, where this is realistic.

In practice, however, it could prove challenging for Humanitarian Organizations to provide Data Subjects with information along the above lines when using Drones to collect Personal Data. Nonetheless, the various options to be decided on a case-by-case basis could include information campaigns, public notices and other similar measures. Drone operators should publish information on their website or on dedicated platforms to inform individuals about the different operations that have taken place as well as forthcoming ones. In remote areas or where it is unlikely that individuals can access the Internet, information can be published in newspapers, leaflets or posters, or provided by means of a letter or radio broadcast.

As far as drone applications that may cover larger geographical areas are concerned, where the provision of information to Data Subjects proves difficult or impossible, the creation of a national or cross-national information resource (easier to trace than websites of single operators) has been suggested to enable individuals to identify the missions and operators associated with particular Drones.

Data Subjects should also have the right to opt out of the Processing, even though this can be challenging in the case of Drones, as individuals might not be able to avoid the surveyed area, or might not even be aware of the data collection through Drone sensors. Furthermore, Humanitarian Organizations are strongly encouraged to implement complaint procedures in their Personal Data Processing practices and internal data protection policies. These procedures should enable data correction and erasure. However, it should be recognized that there may be legal bases for data Processing that do not allow the exercise of all individual rights (for instance, requests for opt-outs by individuals may not be observed in the event of Processing undertaken under the public interest legal basis described above).

Finally, as far as the right to access information is concerned, access should be limited in order to mitigate the risks that access by one Data Subject could expose the Personal Data of other Data Subjects, or that ill-intentioned Data Subjects may take action detrimental to vulnerable individuals, whether identifiable or not.

Limiting access exclusively to aerial imagery or footage including Personal Data of a Data Subject is particularly challenging, since, by its nature, it may include Personal Data of many other individuals and it is highly unlikely that it may be practicably and meaningfully redacted.

EXAMPLE:
In the case of aerial photography collected by Drones, the exercise of the right to access by Data Subjects may require the blurring of other faces or Personal Data not related to the applicant; in the same cases, the right to object could include de-identification of the applicant's Personal Data on the same photograph, but not the destruction of the photograph itself or the Personal Data of other individuals appearing on it.

7.4 DATA SHARING

The circumstances under which personal information is exchanged between Humanitarian Organizations or between Humanitarian Organizations and Third Parties need to be identified and addressed with respect to data protection. Information collected by Drones may be shared either at the moment of collection or at a later stage. Humanitarian Organizations may outsource drone-related work to Data Processors. In the event that any of the above involves Personal Data being shared across national borders, the relevant issues concerning International Data Sharing also need to be addressed.[14]

In these cases, it is important to consider:

- the data protection roles of the Humanitarian Organizations concerned;[15]
- whether imagery or other information exchanged should include Personal Data or whether it is sufficient to share only the conclusions and findings of the analysis and assessment of the imagery collected (no raw data exchange);
- involuntary or accidental data sharing (e.g. if imagery is saved on the device and the device is captured), or if an aerial imagery feed is transmitted in a non-secure and unencrypted way; the impact of this should also be taken into consideration by the Humanitarian Organizations involved.

Crowdsourcing is a common way of Processing and analysing large data sets collected by Drones. Its importance derives from the fact that aerial imagery or footage is often massive and reviewing all this material is impossible for Humanitarian Organizations themselves. An increasingly common practice is to post the imagery online and invite volunteers to review it in order to spot, for instance, interrupted power lines, destroyed houses, affected people, and cattle, etc. However, this can have severe negative consequences (e.g. enabling access to online material by potentially ill-intentioned Third Parties). It is important, therefore, to ensure that:

14 See Chapter 4: International Data Sharing.

15 See Section 7.6 – Data Controller/Data Processor relationship.

- the volunteers accessing the imagery are vetted and trained by the Humanitarian Organization;
- the volunteers commit to a Processing agreement which includes provisions covering discretion and confidentiality;
- the material is not published or otherwise shared beyond the group of vetted volunteers;
- volunteers receive appropriate support to understand the purpose of the data Processing;
- volunteers' Processing is properly logged.

7.5 INTERNATIONAL DATA SHARING

Data protection law restricts International Data Sharing, so Humanitarian Organizations should have mechanisms in place to provide a legal basis for it when Drones are used, as discussed in Chapter 4: International Data Sharing. Humanitarian Organizations should examine whether International Data Sharing has a legal basis under applicable law and in line with their own internal policies before carrying it out. Performing a Data Protection Impact Assessment prior to the International Data Sharing concerned could further strengthen the lawfulness of such Processing.[16]

7.6 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

The roles of Data Controller and Data Processor may be unclear when operating Drones or when Processing data collected by them. As noted, outsourcing is also frequent in Drone-related Processing. It is thus crucial to determine which parties actually determine the purposes and means of data Processing (and thus are Data Controllers), and which parties merely take instructions from Data Controllers (and thus are Data Processors). It is also possible that multiple parties might be considered to be joint Data Controllers.

EXAMPLES:

- A Humanitarian Organization whose own staff operate Drones for its own purposes is the (only) Data Controller for such Processing.
- A Humanitarian Organization outsourcing a Drone operation to a specialized corporation, whose sole task is to pilot the Drones, would be the (only) Data Controller for such Processing; the corporation would be the Data Processor for this operation.

16 See Section 7.7 – Data Protection Impact Assessments.

- Two Humanitarian Organizations who wish to use Drones and outsource all relevant operational work to a corporation having no access to the data collected will be joint Data Controllers. The corporation would be the Data Processor for the operation.

7.7 DATA PROTECTION IMPACT ASSESSMENTS

As discussed in Chapter 5: Data Protection Impact Assessments (DPIAs), DPIAs are important tools used during project design to ensure that all aspects of data protection regulations and applicable risks are addressed. Apart from clarifying the Processing details and specifications, DPIAs should focus on risks posed by the operation as well as on mitigating measures. In this regard, it is important to note that DPIAs should be drafted prior to any Drone operations.

In order to avoid hindering humanitarian operations, template DPIAs for the use of Drones should be developed beforehand. These templates should cover the specific risks and considerations outlined in the present chapter and be easy and quick to complete and implement.